

“Assim como os avanços tecnológicos e a mobilidade têm impactado diretamente o nosso dia a dia, abrindo novas oportunidades e perspectivas, a disseminação de informações também ganhou dimensão ampliada. É nesse contexto que a obra de Patricia Peck Pinheiro tem importância elevada, celebrada nesta 5ª edição especial de 10 anos. O Direito Digital é, para nós, tema recorrente, assim como as questões aqui apresentadas, fazendo crescer esta obra e o nosso conhecimento sobre o assunto.”

Candido Leonelli – Diretor Executivo – Banco Bradesco S.A.

“O mundo interconectado fica mais leve com as orientações jurídicas contidas na obra de Patricia Peck Pinheiro. No tocante ao Direito Digital, tenho recorrido constantemente ao trabalho e à busca incessante desta renomada autora e brilhante advogada. Dessa forma, os riscos ficam diminuídos, as políticas de segurança da informação tornam-se instrumento do dia a dia no mundo empresarial; isto de forma clara, em linguagem que os não juristas entendem com facilidade. Hoje, a Dra. Patricia aborda todos os pontos importantes do Direito Digital, incluindo Transações Comerciais, Redes Sociais, Propriedade Intelectual, Aplicações Móveis, entre outros. Suas orientações em contratos envolvendo relações digitais são fundamentais na vida de um executivo de Tecnologia da Informação.”

José Carlos Padilha – CIO – Carbocloro S.A. – Indústrias Químicas

“À Dra. Patricia Peck, que assim como eu acreditou e enxergou o potencial do mundo ‘digital’ num momento onde todos achavam loucura pensar no assunto e soube concretizar os seus sonhos e projetos de um jeito muito simples: amando o que faz. Parabéns pela sua história, que serve como fonte de inspiração para muitos.”

Clóvis Josué C. Souza – CEO – Giuliana Flores

Patricia Peck Pinheiro

DIREITODIGITAL

DIREITODIGITAL

Patricia Peck Pinheiro

5ª edição

revista, atualizada e ampliada
de acordo com as Leis n. 12.735
e 12.737, de 2012

SAC | 0800-0557688
Jur | saraivajur@editorasaraiva.com.br
De 2ª a 6ª, das 8:30 às 19:30

 **SaraivaJur**
www.saraivajur.com.br O seu portal
jurídico
na Internet

Indicado para:

Profissionais



BSCCSH
210888

34:004
P657d1

5. ed.

Editora
Saraiva

 **Editora
Saraiva**

34.004
P657 d1

Patricia Peck Pinheiro

DIREITODIGITAL

5ª edição

revista, atualizada e ampliada
de acordo com as Leis n. 12.735
e 12.737, de 2012

2013

 **Editora
Saraiva**

Este livro é uma edição especial que celebra os 10 anos da obra *Direito Digital* e a evolução do tema nos últimos anos, no Brasil e no mundo.

Foram trazidas novas questões como BYOD (Bring Your Own Device) nas empresas, a mobilidade ainda maior dos colaboradores, o crescimento do *cloud computing* e das redes sociais, o aumento das discussões sobre privacidade, as recentes mudanças legislativas e seus reflexos na CLT (Consolidação das Leis do Trabalho), a nova Lei de Acesso à Informação, a nova Lei de Digitalização, a nova Lei de Crimes Digitais, bem como os novos entendimentos do Judiciário sobre responsabilidade civil na internet.

Além disso, em razão da importância do Brasil e de sua participação nos grandes eventos esportivos nos próximos anos, há um tópico novo dedicado à análise do tema Segurança Pública Digital e de quais são os desafios do Estado Digital para implementar um plano estratégico de combate às novas ameaças, ao ciberterrorismo, ao crime organizado eletrônico e à guerra cibernética.

A obra foi completamente revista, atualizada e ampliada e voltou a ter modelos e minutas, além de uma seção dedicada a perguntas e respostas mais frequentes do Direito Digital. Por certo, trata-se de livro que irá inspirar os leitores a pensar novas ideias para a Sociedade e o Direito da Era Digital. Boa leitura!

Rua Henrique Schaumann, 270, Cerqueira César — São Paulo — SP
CEP 05413-909
PABX: (11) 3613 3000
SACJUR: 0800 055 7688
De 2ª a 6ª, das 8:30 às 19:30
saraivajur@editorasaraiva.com.br
Acesse: www.saraivajur.com.br

FILIAIS

AMAZONAS/RONDÔNIA/RORAIMA/ACRE

Rua Costa Azevedo, 56 — Centro
Fone: (92) 3633-4227 — Fax: (92) 3633-4782 — Manaus

BAHIA/SERGIPE

Rua Agripino Dória, 23 — Brotas
Fone: (71) 3381-5854 / 3381-5895
Fax: (71) 3381-0959 — Salvador

BAURU (SÃO PAULO)

Rua Monsenhor Claro, 2-55/2-57 — Centro
Fone: (14) 3234-5643 — Fax: (14) 3234-7401 — Bauru

CEARÁ/PIAUÍ/MARANHÃO

Av. Filomeno Gomes, 670 — Jacarecanga
Fone: (85) 3238-2323 / 3238-1384
Fax: (85) 3238-1331 — Fortaleza

DISTRITO FEDERAL

SIA/SUL Trecho 2 Lote 850 — Setor de Indústria e Abastecimento
Fone: (61) 3344-2920 / 3344-2951
Fax: (61) 3344-1709 — Brasília

GOIÁS/TOCANTINS

Av. Independência, 5330 — Setor Aeroporto
Fone: (62) 3225-2882 / 3212-2806
Fax: (62) 3224-3016 — Goiânia

MATO GROSSO DO SUL/MATO GROSSO

Rua 14 de Julho, 3148 — Centro
Fone: (67) 3382-3682 — Fax: (67) 3382-0112 — Campo Grande

MINAS GERAIS

Rua Além Paraíba, 449 — Lagoinha
Fone: (31) 3429-8300 — Fax: (31) 3429-8310 — Belo Horizonte

PARÁ/AMAPÁ

Travessa Apinagés, 186 — Batista Campos
Fone: (91) 3222-9034 / 3224-9038
Fax: (91) 3241-0499 — Belém

PARANÁ/SANTA CATARINA

Rua Conselheiro Laurindo, 2895 — Prado Velho
Fone/Fax: (41) 3332-4894 — Curitiba

PERNAMBUCO/PARAÍBA/R. G. DO NORTE/ALAGOAS

Rua Corredor do Bispo, 185 — Boa Vista
Fone: (81) 3421-4246 — Fax: (81) 3421-4510 — Recife

RIBEIRÃO PRETO (SÃO PAULO)

Av. Francisco Junqueira, 1255 — Centro
Fone: (16) 3610-5843 — Fax: (16) 3610-8284 — Ribeirão Preto

RIO DE JANEIRO/ESPÍRITO SANTO

Rua Visconde de Santa Isabel, 113 a 119 — Vila Isabel
Fone: (21) 2577-9494 — Fax: (21) 2577-8867 / 2577-9565
Rio de Janeiro

RIO GRANDE DO SUL

Av. A. J. Renner, 231 — Farrapos
Fone/Fax: (51) 3371-4001 / 3371-1467 / 3371-1567
Porto Alegre

SÃO PAULO

Av. Antártica, 92 — Barra Funda
Fone: PABX (11) 3616-3666 — São Paulo

197.007.005.001

961826

ISBN 978-85-02-20165-1

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Pinheiro, Patricia Peck

Direito digital / Patricia Peck Pinheiro. — 5. ed. rev.,
atual. e ampl. de acordo com as Leis n. 12.735 e 12.737,
de 2012 — São Paulo : Saraiva, 2013.

1. Internet - Legislação 2. Mídia digital - Leis e
legislação 3. Tecnologia e Direito I. Título.

12-14137

CDU-34:004

Índice para catálogo sistemático:

1. Direito digital

34:004

Diretor editorial Luiz Roberto Curia

Gerente de produção editorial Lígia Alves

Editora Thaís de Camargo Rodrigues

Produtora editorial Clarissa Boraschi Maria

Preparação de originais Ana Cristina Garcia

Maria Izabel Barreiros Bitencourt Bressan

Raquel Benchimol Rosenthal

Arte e diagramação Cristina Aparecida Agudo de Freitas

Isabela Agrela Teles Veras

Revisão de provas Rita de Cássia Queiroz Gorgatti

Ivani A. M. Cazarim

Serviços editoriais Elaine Cristina da Silva

Tatiana dos Santos Romão

Foto Adriana Elias

Capa Vinicius Azevedo Vieira

Produção gráfica Marli Rampim

Impressão Prol Editora Gráfica

Acabamento Prol Editora Gráfica

UFSC - Biblioteca Central

Reg. nº 240888

Data: 24.09.13

Data de fechamento da edição: 4-2-2013

Dúvidas?

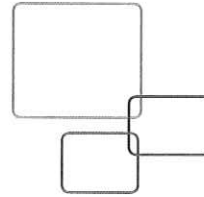
Acesse www.saraivajur.com.br

Nenhuma parte desta publicação poderá ser reproduzida por qualquer meio
ou forma sem a prévia autorização da Editora Saraiva.
A violação dos direitos autorais é crime estabelecido na Lei n. 9.610/98 e
punido pelo artigo 184 do Código Penal.

Dedico este livro ao amor da minha vida, *Romulo Pinheiro*, quem eu conheci por conta de um *e-mail*, em um dia qualquer, e que despretensiosamente acabou se revelando o homem mais fantástico, inteligente e romântico que já conheci, por seu apoio, incentivo, companheirismo e amor.

Dedico este livro também a meus amados filhos, Gabriela e Rafael Pinheiro.

Finalmente, dedico este livro à minha maravilhosa mãe, Jane Peck, à minha querida irmã gêmea, Danielle Peck, a meu querido irmão, Luiz Garrido (codinome ZU), e à minha querida sogra, Maria da Penha Pinheiro, que é como uma mãe para mim.



“Estamos vivendo a era da informação, conectados à internet, com velocidade, com mobilidade, com armazenamento nas nuvens, e permitindo a inclusão digital da população. Neste cenário, a Segurança da Informação passa a ser item de primeira necessidade, que merece toda nossa atenção e adoção de hábitos seguros. Temos que evoluir a nossa cultura e as legislações nesta direção.”

Claudio Laudeauzer — Diretor Corporativo de Tecnologia da Informação — Grupo Fleury.

“Direito Digital é um tema que merece atenção, prioridade e foco de todas as organizações, da sociedade e, principalmente, dos cidadãos nela inserida, pois o uso cada vez mais intenso de diversos recursos tecnológicos nos torna cada vez mais dependentes do mundo digital. Como resultado, várias questões legais surgem e merecem o tratamento adequado tanto na análise, como na busca de solução. Esta nova edição do livro da Patricia Peck traz de uma maneira bem prática as questões jurídicas envolvidas neste novo cenário.”

Jorge Luís Cordenonsi — Diretor de TI para América do Sul e Central — Sodexo

“Este livro consolida um trabalho incansável da Dra. Patricia Peck na pesquisa e apresentação de forma didática todas as legislações e assuntos relacionados ao tema Direito Digital. É leitura obrigatória de todos os empresários e profissionais que trabalham para que nosso país tenha um futuro responsável e muito, muito ‘legal’.”

Norberto Colla — Diretoria de TI e Logística — Angeloni

“Direito Digital” ao longo destes anos tem sido um guia importantíssimo, sempre atualizado, para o desenvolvimento da tecnologia digital (Internet) no Brasil nos aspectos de entendimento jurídico dos novos cenários mesmo sem uma legislação específica. É uma conexão bastante eficaz entre o técnico e o jurídico. Para as empresas um norteador de quais são os novos riscos e de como mitigá-los neste novo mundo cada vez mais interconectado por uma tecnologia em rápido desenvolvimento e adoção pelos usuários.”

Paulo Martins — Diretor de Prevenção a Fraude, Riscos e Segurança da Informação — Telefonica Vivo

“Desde o dia que conheci Patricia Peck e seu trabalho ela tem sido uma colaboradora importante e imprescindível na nossa empresa. Nesta área digital, nova, dinâmica e por isto ainda com tantas dúvidas e incertezas jurídicas contar com o apoio, conselhos e pareceres de Patricia nos dar a segurança de que estamos cumprindo as regras e dentro da ética.”

Olivia Machado — Sócia-diretora — África Publicidade

“A M2SYS TECNOLOGIA como empresa líder e inovadora no Universo de soluções Tecnológicas por Imagem para o mercado financeiro agradece o apoio da consultoria jurídica da Dra. Patricia Peck, com ela temos conseguido transmitir confiança e segurança jurídica aos nossos clientes.”

Marcio Augusto Guariente — Diretor Executivo — M2Sys Tecnologia e Serviços S.A.

“Há dez anos Patricia Peck foi uma das vozes pioneiras do Direito a desenhar o cenário de mudanças que chegavam às empresas por conta da revolução digital, alertando para a necessidade premente da sociedade entender seu impacto nas relações sociais e comerciais. A abrangência e acuracidade da obra a tornam leitura indispensável, especialmente quando, nas nuvens, trafegam dados pessoais e corporativos e as noções sobre o que é público e o que é privado ficam cada vez mais fluidas.”

Silvia Bassi — Presidente e Publisher da Now Digital Business

“A gestão do direito digital nas empresas passou nos últimos anos da última etapa do processo de TI, onde era lembrado apenas quando incidentes de TI ocorriam, passando hoje para o início do processo de planejamento estratégico de TI, ou seja, se transformando num aspecto fundamental a ser considerado nos planos de uso de novas tecnologias no mundo corporativo.”

Manoel Ribeiro — Presidente — Grupo de Gestores de TIC do Ceará

“Patricia Peck escreve com clareza e sabedoria, desmistificando a interface entre o Direito e a Tecnologia. ‘Direito Digital’ é leitura fundamental para quem quer entender como a Tecnologia da Informação tem sido regulada no Brasil nos últimos 10 anos.”

Jorge Fernando Krug, CCSO, Certified Security Officer, PCI, Former Board of Advisors Member Smart Card Alliance Latin America e Caribe — SCALA, Financial Payment Council Leadership Superintendente da Unidade de Segurança de TI — USTI Presidente da Autoridade Certificadora do Estado do Rio Grande do Sul — ACRS — Banco do Estado do Rio Grande do Sul — BANRISUL

“Conheci Patricia Peck em 1999, quando a internet era uma realidade distante para muitas pessoas e empresas; assim, o estudo jurídico dos seus impactos nas relações sociais e empresariais era restrito a alguns poucos visionários, que perceberam que, inevitavelmente, essa tecnologia iria adentrar nossas vidas e lares, modificando definitivamente a forma de nos relacionarmos com tudo. Mais do que uma visionária, Patricia é uma apaixonada pelo tema, paixão essa que transmite com clareza como profissional e em seus livros. ‘Direito Digital 5.0’ traz o equilíbrio perspicaz entre educação e segurança, direitos e deveres, doutrina e a prática jurídica nesse universo virtual!”

Eduardo Augusto Marcondes de Freitas — Advogado Sênior da Diretoria Jurídica da Federação Brasileira de Bancos

“Neste livro extraordinário e didático, a Dra. Peck dissemina sua notória cultura de segurança integrada e holística, essencial para a proteção de negócios na era digital. Neste novo ambiente de nuvem e mobilidade, a empresa não detém mais total controle sobre seus dados — eles estão circulando continuamente e, por isso, esta obra colabora para que as instituições possam — por meio de ações concretas de governança corporativa — orientar, normatizar, monitorar e agir rapidamente em caso de incidentes.”

Paulo Pagliusi — Diretor da Cloud Security Alliance Brasil (CSABR) e ISACA Rio de Janeiro (ISACA-RJ), é Sócio da Procela Inteligência em Segurança. Capitão de Mar e Guerra da Reserva (Marinha), foi Diretor (CEO) de duas Organizações Militares e fundou a Divisão de Criptologia (CASNAV). Ph.D. in Information Security pela Royal Holloway, University of London, Mestre em Computação pela UNICAMP, possui certificações CISM e BS7799 Lead Auditor

“A presença do Direito Digital em nossas vidas é inexorável, o que atrai a sua imprescindível doutrinação para delinear os limites, apontar os riscos e sugerir o ambiente de segurança que as pessoas necessitam para proteger as suas informações privadas e sensíveis. Esta obra cumpre este propósito, pois propicia o conhecimento dos direitos, o que facilita o seu exercício.”

Josenir Teixeira — Advogado, Mestre em Direito — Diretor Jurídico da Pró-Saúde ABASH

“O universo digital está cada vez mais presente no dia a dia das pessoas e, por mais virtual que possa parecer, as empresas devem percebê-lo como algo real e concreto, considerando todo o espectro de ameaças e de benefícios. O modo como as novas tecnologias impacta o cotidiano e os negócios, nos coloca diante de uma realidade completamente nova e nos obriga a aprender a lidar com elementos como a privacidade, por exemplo, de maneira diferente da qual estamos acostumados. Neste sentido o trabalho de Patricia Peck representa uma grande contribuição para refletirmos sobre este tema, inclusive no que diz respeito a ética.”

Gabriela Baumgart — Diretora de Marketing — Shopping Center Norte

“Nesse livro indispensável, a Dra. Patricia Peck aborda e esclarece com maestria — e de forma clara, sem deixar de lado a técnica — sobre o Direito Digital, matéria que é fundamental nos dias atuais, face presença crescente (e inexorável) da vida cibernética dentro do dia a dia de cada um de nós. Leitura obrigatória e deliciosa!”

Álvaro Loureiro — Diretor Jurídico — Banco Bonsucesso S/A

“A presença corporativa em redes sociais depende da estratégia de comunicação da organização, e deve ser muito bem planejada e estruturada de acordo com os públicos de relacionamento. Um dos desafios é acompanhar a evolução e a inovação do mundo virtual em sinergia com as novas gerações; outro é fazer-se presente, em sintonia com os princípios legais e normas que permeiam a relação no âmbito digital.”

Fabiane Caldi — Advogada — Grupo Boticário

“O livro Direito Digital tornou-se uma das obras de referência para a Segurança da Informação no Brasil. Sempre atualizado e com uma linguagem acessível, consegue traduzir a complexidade técnica das ameaças digitais de forma clara para o ambiente jurídico e vice-versa, trazendo também para os profissionais e gestores técnicos de TI a visão e os aspectos legais envolvendo estas mesmas ameaças.”

Marcelo Figueiredo — Gerente de Infraestrutura e Segurança da Informação — Grupo SBF

“As lições da Dra. Patricia Peck a respeito das várias questões nascidas do moderno direito digital, além de contribuírem para o aprimoramento da jurisprudência dos Tribunais brasileiros, são uma importante ferramenta no âmbito empresarial. Posso afirmar que a advogada Patricia Peck é uma referência nos temas que envolvem a internet.”

Mônica Lanat Silveira, Gerente-Geral Jurídico da Infoglobo Comunicação e Participações S.A.

“É fato inegável que a tecnologia da informação vem, cada vez mais, influenciando o comportamento da sociedade moderna. Chats, blogs, redes sociais, compras on-line, Internet banking e tantas outras tecnologias já foram incorporadas massivamente na rotina das pessoas e das empresas. E o ordenamento jurídico tem papel fundamental nesta evolução ao ditar as regras para este novo modelo de sociedade. Esta obra, de valor inestimável que agora completa 10 anos, vem cumprindo com pleno êxito sua missão de difundir novos conceitos sob o ponto de vista legal, sendo indispensável para qualquer pessoa que encontra-se imersa no mundo virtual.”

Yanis Cardoso Stoyannis — Gerente de Segurança da Informação — Embratel

“A experiência da Patricia Peck em Direito Digital, demonstrada e comprovada nos últimos anos, reforça ainda mais o valor de suas recomendações nesta 5ª edição da obra Direito Digital. Um excelente guia para ajudar as empresas em seus desafios tecnológicos diários, que geram muitas oportunidades mas também muitos riscos.”

Denise Comerlati Menoncello — Gerente Corporativo de Segurança da Informação — Serasa Experian

“A era digital nos instiga a novos desafios. A linha entre o legal e o ilegal, o ético e o inoportuno fica cada vez mais tênue. Recorremos ao conhecimento e a prática de Patricia Peck para aperfeiçoar o modelo de gestão da informação do Centro de Memória Bunge, tornando-o mais seguro, democrático e menos burocrático. Sabemos, no entanto, que este é um desafio permanente pois os avanços tecnológicos estão e sempre estarão desafiando o conjunto da sociedade.”

Juliana Santana — Gerente de Responsabilidade Social da Fundação Bunge

“A era digital fez com que as empresas mudassem substancialmente sua forma de atuação junto aos seus clientes e fornecedores, fato esse que exige do advogado de empresa conhecimento específico e constante atualização em Direito Digital.”

Elaine Gadelha Barros — Gerente Jurídica — Natura Cosméticos S.A.

“A mobilidade e o avanço crescente da tecnologia da informação alteraram, e vem alterando, as relações sociais e jurídicas. A relativização do princípio da cartularidade do título judicial e as relações contratuais virtuais são alguns dos temas mais discutidos. Esta nova edição da obra Direito Digital vem, de forma clara e eficiente, abordar e esclarecer temas de grande relevo, a exemplo dos acima citados. Trata-se de obra essencial não só para os profissionais da área do Direito, mas para toda a sociedade.”

Jean Marcell de Miranda Vieira — Gerente do Ambiente Jurídico de Gestão do Contencioso — Banco do Nordeste

"A obra apresenta conteúdo de vital relevância sobre a fronteira viva entre o direito e os novos desafios da era digital. A obra é imprescindível referência para o tema, suscitando reflexões fundamentais sobre o ordenamento jurídico e sua interseção com as práticas modernas e dinâmicas das tecnologias contemporâneas. A consistência do posicionamento da autora sedimenta o "Direito Digital" como um marco na literatura especializada."

Ricardo Fanfa Capaverde — Gerente — Caixa Econômica Federal

"Independente da área de atuação é imprescindível que o advogado esteja atualizado em matéria de direito digital, já que esta se correlaciona com as demais áreas do direito. Muito mais que um livro sobre direito digital, este é um notável vade mecum que deve ser usado para melhor entender e aprender sobre a maioria das questões jurídicas numa época em que a tecnologia está inserida no cotidiano de todos, no qual a Dra. Patricia, de forma brilhante, ilustra com tanta capacidade."

Claudia Carvalho Valente — Gerente Jurídica — Adidas do Brasil

"Falar sobre a importância do Direito Digital nas organizações, para nós gestores, é como falar sobre a alta disponibilidade dos serviços de Tecnologia. Este assunto tornou-se o alicerce de qualquer Governança em TI e a sua importância é tão fundamental como ter a internet ligada, o celular funcionando, faz parte do nosso dia a dia. Gerir novos riscos tais como ter um novo acesso, uma rede social imprescindível ao negócio, uma tecnologia inovadora faz com que a Gestão de TI tenha que disponibilizar estes recursos com rapidez e tranquilidade. Nós da ABBrazil o fazemos pois temos total alinhamento e atualização do Direito Digital, pois para nós este assunto esta no DNA da empresa e correr riscos se torna desnecessário."

Eliane Serrano — Gerente de Informática — ABBrazil

"Com maestria, humor e muita competência, a Dra Patricia Peck aborda as disciplinas de Segurança da Informação e Direito Digital de forma clara, profunda e prática e nos brinda com um livro completo e atual e que já é considerado uma referência nesta área."

Ana Lucia de Queiroz Tourinho — Gerente de Tecnologia da Informação da Emulzint e Professora de Pós-Graduação do IBE-FGV.

"O Direito Digital é mais um conhecimento que os gestores de TI devem adquirir, pois existem leis que desconhecemos, como por exemplo a "Territorialidade dos dados" citado em artigos publicados pela Dra. Patricia Peck."

Eduardo Lucas Pinto — Gerente de TI — Colégio Dante Alighieri

"Hoje a mobilidade propicia as pessoas estarem conectadas 24 horas por dia, sete dias na semana, o que agiliza em muito no trabalho e no relacionamento nas redes sociais as trocas de conhecimento e a atualização das informações, mas isso tem impactos em nossa nova sociedade e nas relações de trabalho. E ainda mais, os riscos de segurança da informação pessoais e corporativos na internet. Ninguém está preocupado em proteger seus dados, falta consciência dos impactos que a falta de privacidade pode trazer para as pessoas, para as corporações na utilização das novas tecnologias."

Carlos Eduardo de Oliveira Gambôa — Gerente de Tecnologia da Informação — FIRJAN

"A Dra. Patricia Peck e sua obra vêm sendo tão fundamentais para o crescimento da internet no Brasil quanto as inovações tecnológicas e sociais que ela busca explicar sob o ponto de vista jurídico. Este livro foi pioneiro em seu lançamento e continua sendo um guia importante para empresas, instituições e profissionais."

Guilherme Mazzola — Gerente de Marketing de Produtos da Locaweb

"Há uma tendência natural dos profissionais envolvidos com Segurança da Informação de manter uma certa distância de assuntos jurídicos, por desconhecimento da matéria, e, com isto, muitas vezes se acham em situações de dificuldade diante dos problemas do dia a dia, por não saber se proteger adequadamente, com antecedência, nem como agir, quando as situações jurídicas se apresentam. A Dra. Patricia Peck consegue costurar um amplo conhecimento técnico das novidades do mundo da Internet com as complexidades do mundo jurídico. Recomendo essa leitura para todos os profissionais de Segurança da Informação."

Alfred John Bacon — CISSP, CISA, CISM, CRISC — Consultor Sênior da Petrobras e Presidente do Capítulo ISACA Rio de Janeiro

"Conhecimento. Esta palavra resume o que se obtém com a leitura do conteúdo desta obra. Leitura esta que é essencial para aqueles que querem aplicar as práticas do Direito Digital na promoção da Segurança da Informação nas Organizações. É uma obra de grande valia que tem trazido bons resultados para a esfera pública."

Elba Vieira — Assessora-Chefe de Segurança Integrada — Cia. de Processamento de Dados do Estado da Bahia (PRODEB)

"As instituições educativas, especialmente as que carregam em sua identidade a marca da excelência na formação, não podem entender seu trabalho fora do espaço das mídias sociais e das novas tecnologias. Não obstante, mais do que equipar salas de aula com novos e modernos equipamentos ou oferecer aos estudantes ferramentas inovadoras para o processo de aprendizagem, o desafio que se apresenta é a dimensão

ética no uso de tantos e tão diversificados recursos. O conhecimento na área de direito digital só fará diferença na educação se possibilitar (tal como na obra em questão) a reflexão sobre os valores que qualificam a vida e as relações das pessoas. Quando a apropriação do marco legal é feita a partir do referencial ético, a escola pode contar com elementos para a construção de relações fraternas, justas e solidárias que ultrapassem os limites do referencial normativo que a informação sobre a lei oferece.”

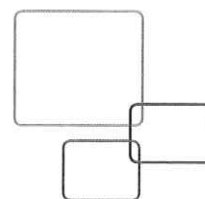
Sônia M. V. Magalhães — Articuladora Nacional da Área de Educação Básica — Rede Jesuíta de Educação

“No contexto da permanente evolução tecnológica, seria ingênuo acreditar não caber ao gestor o estudo amplo e atualizado das questões relacionadas ao Direito Digital. Neste aspecto, o livro nos ajuda a entender e construir uma cultura de proteção do conhecimento e da reputação, independente da qualidade do dispositivo tecnológico envolvido, particular ou corporativo. De forma pragmática, a obra correlaciona diversas atividades cotidianas da empresa com a legislação aplicável, contribuindo assim para o aprimoramento de contratos, políticas, regulamentos e procedimentos internos. Brilhantemente, a autora elucida os novos riscos a que estamos sujeitos na Sociedade da Informação, seja como empresa ou cidadão.”

Claudio Barbosa — Analista de Gestão — Sabesp

“Na realidade digital em que vivemos, é impossível contribuir para a sobrevivência de uma organização, com a segurança que o Direito Digital oferece, sem o conhecimento do conteúdo desta publicação.”

Graça Bahia — Bibliotecária — Construtora Norberto Odebrecht S/A.



Agradecimentos

Esta 5ª edição é muito especial, pois comemora os 10 anos da obra e do crescimento do Direito Digital no Brasil e no mundo. De uma novidade no meio jurídico no início, este assunto tornou-se essencial na vida das pessoas e nas empresas, tratando de temas que vão da segurança digital até como educar os filhos a ter postura ética nas redes sociais.

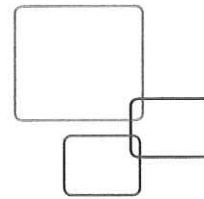
Agradeço à minha família, em especial a meu marido, Romulo Pinheiro, que é meu muso inspirador e que me motivou a criar um escritório de advocacia com foco em Direito Digital, Inovação e Gestão de Riscos.

Agradeço em especial à jovem advogada Rebeca Arima, responsável por me ajudar na revisão e atualização desta edição, bem como aos meus inestimáveis sócios, em especial a Sandra Tomazi, Leandro Bissoli, Victor Haikal, Isabela Guimarães, Luiz Henrique Souza, Diego Almeida e Gisele Arantes, bem como à brilhante equipe que tenho no escritório e que permite que o tempo se multiplique e que possamos juntos encontrar respostas e pensar soluções para os novos desafios trazidos pela Sociedade do Conhecimento, conectada e sem fronteiras.

Esta obra reúne o que há de melhor no pensamento estratégico do Direito Digital, que amadureceu muito, como eu, nestes últimos anos, continuando a inspirar os novos profissionais que estão no início da carreira, além daqueles que já têm anos de experiência e buscam atualização. Esta obra está e estará sempre em constante evolução, pois, quando a sociedade muda, o direito também deve mudar para evoluir junto com ela.

Obrigada,

Dra. Patricia Peck Pinheiro



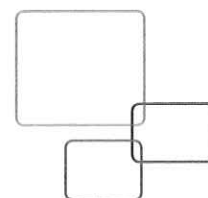
Índice

<i>Agradecimentos</i>	15
<i>Prefácio à 5ª Edição</i>	21
<i>Prefácio à 4ª Edição</i>	25
<i>Prefácio à 3ª Edição</i>	29
<i>Prefácio à 2ª Edição</i>	35
<i>Prefácio à 1ª Edição</i>	39
<i>Nota da Autora — O Direito Digital em Transformação</i>	41
1. Introdução	47
2. Da invenção do rádio à convergência de mídias: os reflexos comportamentais das mudanças tecnológicas	51
3. Os conceitos que constituem a estrutura fundamental do pensa- mento jurídico	55
4. Rumo à sociedade digital	59
5. Sociedade digital	67

6. A evolução do Direito.....	73
7. Direito Digital.....	75
7.1. O elemento tempo.....	81
7.2. Territorialidade.....	82
7.3. Direito à informação e à liberdade de pensamento.....	85
7.4. Privacidade e anonimato.....	86
7.5. Identidade digital.....	93
7.6. Direito comunitário e direito individual.....	95
7.7. Conciliação e enfrentamento.....	102
7.8. Autorregulamentação.....	103
8. Novos institutos jurídicos de Direito Digital.....	105
8.1. Empresas virtuais e tendências da nova economia.....	105
8.2. Provedores de acesso, de serviços e de conteúdos.....	113
8.3. Comércio eletrônico e <i>e-Business</i>	116
8.4. Consumidor <i>online</i> e o CDC à luz do Direito Digital.....	125
8.5. O <i>e-Business</i> para as Classes C e D — baixa renda.....	134
8.6. O Social-SAC nas redes sociais.....	139
8.7. Propriedade intelectual e o direito autoral nas novas mídias.....	141
8.8. Domínios.....	149
8.9. Proteção de conteúdos, <i>websites</i> e outros direitos autorais digitais.....	159
8.10. Aspectos legais do <i>software</i>	166
8.11. As ferramentas de trabalho tecnológicas — correio eletrônico e outros.....	173
8.12. Segurança da Informação e as ISOs 27002, 18044 e 27001.....	179
8.13. Aspectos legais do monitoramento.....	197
8.14. Aspectos legais do BYOD e a mudança da CLT.....	207
8.15. Documentos eletrônicos.....	212
8.16. Prova eletrônica.....	215
8.17. Assinatura digital e certificação digital.....	222

8.18. Aspectos legais da biometria.....	225
8.19. Computação forense e a perícia digital.....	230
8.20. Leilão virtual.....	236
8.21. Pregão eletrônico.....	241
8.22. Finanças virtuais e o <i>Internet Banking</i>	242
8.23. Aspectos legais do <i>Home Broker</i>	247
8.24. <i>Mobile Banking</i> e <i>Social Banking</i>	251
8.25. Aspectos legais da terceirização em TI (<i>Outsourcing</i>).....	259
8.26. Aspectos legais do <i>cloud computing</i>	261
8.27. As novas regulamentações — Sarbanes-Oxley e Basileia II.....	264
8.28. Tributos.....	268
8.29. Fisco Digital — do SPED à Nota Fiscal Eletrônica.....	278
8.30. <i>E-Government</i> e a Administração Pública na Era das Redes Sociais.....	280
8.31. Justiça Digital — Processo Eletrônico.....	293
8.32. Saúde Digital — Prontuário Eletrônico.....	297
8.33. <i>E-Learning</i>	300
8.34. Aspectos legais do EAD.....	304
8.35. Crimes eletrônicos.....	305
8.36. A fraude eletrônica e os perfis falsos.....	321
8.37. A legítima defesa na Internet.....	329
8.38. Publicidade <i>online</i>	333
8.39. A questão do <i>spam</i> e do <i>e-mail</i> marketing.....	336
8.40. Acessibilidade.....	343
8.41. Comunidades <i>online</i> , <i>blogs</i> e <i>fotologs</i>	349
8.42. Internet móvel.....	356
8.43. TV Interativa e TV Digital.....	357
8.44. VoIP.....	362
8.45. <i>Web 2.0</i> — redes sociais e seus impactos.....	365
8.46. Monitoramento da Marca na Internet.....	375
8.47. E-Política — aspectos legais das eleições na Internet.....	378
8.48. Espionagem eletrônica.....	388
8.49. <i>Paper less</i> e Gestão Eletrônica de Documentos — GED.....	395

8.50. Seguro de risco eletrônico	402
8.51. Segurança pública digital	405
9. Responsabilidade civil e dano moral no Direito Digital	411
10. Ética e educação digital	423
11. Os principais tipos de usuários de tecnologia e seus impactos no Direito	429
12. Contratos na Era Digital e os contratos específicos de TI	433
13. Boas práticas para SLA — <i>Service Level Agreement</i>	441
14. Arbitragem	449
15. O novo profissional do Direito	453
<i>Referências</i>	461
<i>Glossário</i>	483
<i>FAQ — Perguntas e respostas sobre Direito Digital</i>	503
<i>Modelos de documentos</i>	521
<i>Jurisprudências relacionadas ao Direito Digital</i>	549



Prefácio à 5ª Edição

Mais uma vez Patricia Peck Pinheiro brinda o leitor com uma obra primorosa e instigante a respeito da rápida e ao mesmo tempo preocupante evolução do mundo digital. São inovações e tendências tecnológicas e sociais que a autora apresenta sob o enfoque jurídico, favorecendo a compreensão dos novos cenários e das relações pessoais e comerciais decorrentes das transformações digitais. Com uma linguagem dinâmica, leve e descontraída, a advogada-escritora procura trazer à reflexão temas atuais e conjunturais e assuntos do cotidiano do homem comum. Com profundidade e naturalidade, são tratadas questões como o uso da informação, a espionagem e fraude eletrônica, os aspectos legais das eleições na *internet* — *e-política* —, o comércio eletrônico, os direitos do consumidor *online*, a educação digital, entre outras.

Desde o seu lançamento, há dez anos, *Direito Digital* tem se tornado referência e leitura imprescindível para profissionais de diversificadas áreas. Agora, nesta 5ª edição, o livro se atualiza e se amplia, adequando-se ao novo contexto social e normativo, nacional e internacional. Traz reflexões sobre o forte crescimento das redes sociais e seu impacto nas relações entre indivíduos e empresas, acarretando riscos e oportunidades e favorecendo o surgimento de políticas de uso mais claras e objetivas.

Outro aspecto evidenciado é a necessidade de adaptação estratégica das organizações para lidar com a chamada “Geração Y” e com suas formas de se relacionar com a tecnologia, o meio ambiente e as causas sociais. A autora ressalta a revolução tecnológica representada pela mobilidade, que é capaz de

atingir o dia a dia das pessoas, modificando suas rotinas e formas de tomar decisões, refletindo-se, até mesmo, nas relações de trabalho. Essas tecnologias também afetam as corporações que, cada vez mais, necessitam ter acesso, em tempo real, às informações que lhes permitam decisões oportunas e objetivas.

E não para por aí. O livro apresenta novas nuances sobre os temas relacionados à Privacidade, às Redes Sociais, ao Comércio Eletrônico e *e-Business*, ao Consumidor *Online*, à Propriedade Intelectual, aos Domínios, às Ferramentas Tecnológicas de Trabalho, à Segurança da Informação, à Prova Eletrônica e às Finanças Virtuais. **A necessidade diária que as pessoas têm de otimizar o tempo e de realizar tarefas de modo rápido e eficiente faz com que, cada vez mais, indivíduos e organizações realizem transações financeiras por meio de dispositivos móveis como *Internet Banking*, *Mobile Banking* e *Social Banking*.** A autora, com base em aspectos técnicos e legais, enfatiza a importância da adoção de cuidados e de medidas de segurança na utilização desses serviços.

A obra aborda, ainda, os aspectos legais da *Cloud Computing*, do *e-Government* e da Administração Pública na Era Digital. Patricia Peck alerta sobre o crescimento e a evolução das atividades *online* relacionadas ao governo, sobre os ataques de negação de serviço sofridos e sobre as formas de prevenção e de superação das vulnerabilidades, com base nos recursos de segurança da informação.

A respeito do tema Justiça Digital — Processo Eletrônico, Crimes Eletrônicos, Comunidades *Online*, *Blogs* e *Fotologs*, Web 2.0 — são abordadas a pirataria, a publicação descontrolada de conteúdos na *web* e a Lei de Direitos Autorais. As preocupações, nesse caso, são com a proteção de conhecimentos e inovações; com a garantia da segurança jurídica, em meio a um mundo digital sem fronteiras; com a necessidade de regras, autorregulamentação e leis que viabilizem soluções técnicas e jurídicas; e com a preservação da imagem, da privacidade e da reputação, pois são direitos difíceis de serem assegurados diante desta era de exposição, transparência e falta de controle.

Direito Digital, nesta edição especial, surpreenderá o leitor com um capítulo dedicado à Segurança Pública Digital e à Guerra Cibernética, alertando para a necessidade de vigilância contínua para proteger sistemas críticos, em um contexto em que o controle do ciberespaço é disputado a todo custo. Esta 5ª edição inova, ainda, ao incluir um capítulo com um FAQ — *Frequently Asked Questions* —, possibilitando ao leitor um meio rápido de obter respostas às suas dúvidas e seus problemas.

Outra novidade é um capítulo que compendia doze anos de jurisprudências consolidadas pelo Judiciário Brasileiro, relacionadas ao tema Direito

Digital. Há um novo capítulo com um enfoque mais prático, que apresenta modelos de cláusulas para contratos de tecnologia, cessão de direitos de imagem, contratação eletrônica, cessão de direitos autorais, entre outros. Igualmente, foram tratadas com maior profundidade as questões da Responsabilidade Civil na Internet e da situação do profissional do Direito, em um momento em que se discute, no BRASIL e no mundo, um marco regulatório para a utilização da Internet.

O sucesso desta edição é fruto de conhecimento, competência e larga experiência acumulada ao longo de uma vida dedicada ao Direito e às implicações da Tecnologia nas relações humanas. Desde a adolescência, Patricia Peck Pinheiro já dava sinais de sua incomum capacidade e vocação, quando, aos treze anos, começou a estudar tecnologia, e foi programadora de jogos para computador, tendo tido como seu primeiro videogame um Atari. Iniciava-se, assim, uma carreira brilhante de relevantes contribuições para a sociedade.

Patricia Peck Pinheiro é advogada formada pela Universidade de São Paulo, com especialização em negócios pela Harvard Business School, MBA em *marketing* pela Madia Marketing School e com capacitação em inteligência e contrainteligência pela Escola de Inteligência Militar do Exército. Possui especialização em Gestão de Riscos pela Fundação Dom Cabral. Foi condecorada pelo Exército Brasileiro com as medalhas do Pacificador e Ordem do Mérito Militar. Pela Marinha do Brasil, foi agraciada com a Medalha Mérito Tamandaré. Recebeu os prêmios “Advogada mais Admirada em Propriedade Intelectual no Brasil” (2011 e 2012), “A Nata dos Profissionais de Segurança da Informação” (2006 e 2008) e “Excelência Acadêmica — Melhor Docente — FIT Impacta SP” (2009 e 2010). É autora do livro *Direito Digital* e coautora da obra coletiva *Direito Digital Aplicado*, bem como do audiolivro e do *pocket book* *Direito Digital no Dia a Dia*, *Direito Digital Corporativo* e *e-Eleições*, além de participação nos livros *Direito e Internet II*, *e-Dicas* e *Internet Legal*. É colunista do *Conta Corrente*, da *GloboNews*, do *IDG Now* e articulista do *Valor Econômico*, *Revista Visão Jurídica*, *Revista Partner Sales*, entre outras. Possui experiência internacional nos EUA, Portugal, Coreia. É conferencista do Centro de Inteligência do Exército (Brasília-DF) e da Escola de Inteligência Militar do Exército (Brasília-DF). Já capacitou, em doze anos, mais de cento e cinquenta mil profissionais nos temas relacionados à Conscientização de Segurança da Informação e Boas Práticas de Direito Digital. Ministrou cursos em diversos órgãos da administração pública, dentre os quais, STF, STJ, STM, TST, TCU, Câmara dos Deputados, Ministério da Defesa, INCRA, ELEKTROBRAS, PETROBRAS, BNDES, CNI, SEBRAE, SENAI, FIESP e SENAC. Já ministrou aulas na pós-graduação do SENAC-SP, Impacta, IBTA,

Fatec-SP, LFG, ESPM, USP-ECA, assim como realiza treinamentos *in company* para diversas empresas.

Principal referência em Direito Digital no país, a advogada é a vencedora do Prêmio “Security Leaders” de 2012, na categoria “Campanhas para Conscientização sobre Segurança da Informação”, por conta das ações desenvolvidas e pelo Movimento Família Mais Segura na Internet, projeto idealizado pela profissional.

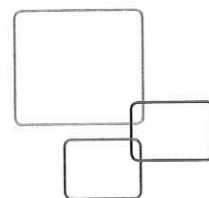
É sócia-fundadora do Escritório Patricia Peck Pinheiro Advogados, especializado em Direito Digital, com matriz localizada em São Paulo. Seus profissionais são especializados em Gestão de Risco, Segurança da Informação, Contratos, Direitos Autorais, Contencioso Corporativo, Análise de *e-Business* (Portais, *Sites*, Mobilidade, entre outros), Comunicação e Promoção, Capacitação e Treinamentos. Atende mais de cento e trinta clientes na América Latina (como o Brasil), nos EUA e em alguns países da Europa.

Esse magnífico currículo não esgota todas as suas capacitações, funções exercidas, trabalhos realizados e reconhecimentos auferidos.

Exultante, mas não surpreso, tendo em vista a qualidade de seus trabalhos, cumprimento a autora pela excelência e pelo primor na concepção desta obra, e agradeço pelos ensinamentos e pela forma amigável com que traduz temas, aparentemente complexos, em assuntos palpáveis e contextualizados com a realidade que circunda o cotidiano de todos nós, sejamos ou não profissionais do Direito.

Boa leitura a todos!

General de Divisão Edson Leal Pujol
Chefe do Centro de Inteligência do Exército



Prefácio à 4ª Edição

“Quanto mais compreendemos sobre o mundo, quanto mais profundo nosso conhecimento, mais específico, consciente e articulado será nosso conhecimento do que ignoramos — o conhecimento da nossa ignorância. Essa, de fato, é a principal fonte da nossa ignorância: o fato de que o nosso conhecimento só pode ser finito, mas nossa ignorância deve necessariamente ser infinita.”

Karl Raimund Popper¹

É sempre útil relembrarmos as memoráveis lições do mais famoso filósofo austríaco do século XX: Karl Raimund Popper. Com a propriedade que lhe é peculiar, Popper ressalta que quanto mais aprendemos sobre o mundo, melhor compreendemos o quão infinita é a nossa ignorância.

E para muitos o Direito Digital ainda é um mistério a ser desvendado.

Há alguns anos venho acompanhando o trabalho inovador e pioneiro da Dra. Patricia Peck nesse novo ramo do Direito, o Direito Digital ou Direito Virtual. Sinto-me, pois, especialmente honrado em prefaciar esta 4ª edição, apenas alguns meses após o lançamento da 3ª edição.

1. *Conjecturas e refutações*, tradução de Sérgio Bath, 5ª ed., Brasília: Editora Universidade de Brasília, 2008, p. 57.

O estudo do Direito sempre é enriquecido quando nos deparamos com obras como esta, sendo um grande privilégio lançar essas palavras preambulares.

Uma vez iniciada a leitura desta obra, o leitor logo perceberá que se trata de um trabalho denso e percuciente, repleto de informações e reflexões que somente um especialista na área do Direito Digital poderia conceber.

E nessa abordagem precisa sobre o Direito Virtual, a autora navega com desenvoltura e propriedade por diversas outras áreas, como o Direito Penal, o Direito Administrativo, o Direito Tributário, entre outras.

Demonstra a ilustre autora intimidade com particularidades afetas a diversas transações e negócios praticados nos Mercados Financeiro e Bursátil, o que torna a presente obra uma leitura indispensável para aqueles que militam nas áreas financeira e de mercado de capitais.

Merece destaque, ainda, a abordagem preciosa que a autora faz sobre a fraude eletrônica e os crimes eletrônicos, tópicos esses revistos e atualizados nesta nova edição, com destaque para a indicação do vácuo legislativo sancionador existente no Brasil para esses crimes.

Como bem lembra a Dra. Patricia Peck no Capítulo 8, item 28, nosso País é conhecido e reconhecido como o maior exportador de crimes eletrônicos do mundo.

Recente matéria publicada no Jornal *Folha de S. Paulo*² corrobora essa informação. Nela, menciona-se que o Brasil também é o campeão mundial de *spams*, “tendo sido a origem de 14% do lixo virtual que entupiu caixas de *e-mails* pelo mundo nos dois primeiros meses do ano”, seguido da Índia com 11%. E de acordo com a matéria, a fraude bancária é o principal foco.

O enquadramento das condutas delituosas praticadas na Era Digital, nos tipos penais descritos no Código Penal de 1940, consubstancia uma tarefa extremamente árdua para os aplicadores do Direito, para dizer o mínimo. É absolutamente imperativo que o Congresso Nacional cumpra o seu dever constitucional e legisle sobre essa matéria, de forma a suprir essa lacuna normativa, haja vista que os índices acima apontados e a impunidade nos envergonham perante a comunidade internacional.

Não bastassem esses pontos brilhantemente expostos na 3ª edição, a autora adiciona na 4ª edição nove novos temas de grande interesse, dentre os quais destacamos: a “Identidade Digital”, o “*e-Business* para as Classes C e D — Bai-

xa Renda”, o “Fisco Digital — *Sped* e Nota Fiscal Eletrônica” e o “Judiciário Digital — O Processo Eletrônico”.

Cabe ressaltar, por derradeiro, que são raras as boas obras sobre o Direito Digital no Brasil, o que valoriza ainda mais o livro da Dra. Patricia Peck, cuja qualidade e profundidade são latentes.

Em face dessas e de outras qualidades que o observador mais atento certamente encontrará na presente obra, cabe-me recomendar com muita segurança a leitura desta quarta edição.

Saúdo e parabeno a ilustre autora.

São Paulo, abril de 2010.

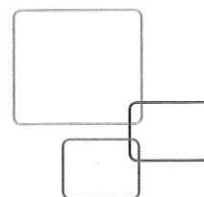
Antonio Carlos de Toledo Negrão

Diretor Jurídico da Federação Brasileira de Bancos — FEBRABAN.

Mestrado em Direito Econômico e Financeiro pela Faculdade de Direito da Universidade de São Paulo.

Especialista em Direito da Empresa e da Economia pela Fundação Getúlio Vargas.

2. Edição de 25-3-2010, matéria de Luciana Coelho, de Genebra.



Prefácio à 3ª Edição

Há tempos venho me permitindo criticar, de forma até certo ponto áspera, os prefácios dos livros que tenho lido — e, por mais incrível que possa parecer, também daqueles que tenho escrito —, convencido que estou da função absolutamente secundária (ou quase mesmo anódina...) que esses textos exercem no espírito dos leitores.

Na grande maioria dos casos, com efeito, eles se limitam a apresentar o autor como se se tratasse de um “atestado de bons antecedentes intelectuais” deste, subscrito por uma pessoa supostamente mais conhecida do público, no caso, o prefaciador...

O caráter meramente laudatório desses prefácios, feitos sob encomenda, torna sua leitura quase sempre sensaborona e de pouca serventia — ou mesmo nenhuma — ao leitor. O próprio apresentador, cômico de que se trata de algo indisfarçavelmente inócuo, acaba se perdendo em parcas justificativas desse seu tosco papel de “mestre de cerimônia com voz enrouquecida” e lança esparsamente dados biográficos do autor com o propósito de dar àquela tarefa algum tipo de utilidade, seja para que o leitor extraia possíveis paralelismos entre o autor e sua obra produzida, seja para que a demonstração de proximidade com a vida do apresentado sirva para justificar a razão de ter sido ele o escolhido para prefaciá-lo... Tudo muito grotesco, afinal de contas, para dizer-se o mínimo...

Escuso-me de pormenorizar aqui os critérios pessoais dos quais tenho me servido para aceitar o encargo de fazer alguns poucos prefácios e de recusar numerosos outros. E o faço pela simples e boa razão de não me compadecer

com os discursos *pro domo* que um certo tipo de pedanteria didática se esforça por institucionalizar no meio acadêmico. De resto, é preciso dizer que muitas de minhas recusas não decorreram de eventuais deficiências da obra a ser apresentada. Ocorreram, na verdade, por limitações exclusivamente minhas... Não é fácil — para quem luta, desesperada e perdidamente, contra a insuficiência de tempo para dar conta de todas as responsabilidades assumidas —, aceitar novos encargos, especialmente quando se sabe, de antemão, que deles não poderemos nos desincumbir com um mínimo de grandeza, como aliás ocorre, lamentavelmente, no presente prefácio...

Acresce existir, no meu caso, o cansaço natural de quem já é obrigado a viver julgando o tempo todo, seja como magistrado, seja como professor. E escolher o que se vai prefaciá-lo e o que não se vai é mais um exercício de julgar do que de qualquer outra coisa. Julgar, em última análise, significa *cortar*, parecendo ser mais atividade de médico-cirurgião — profissão que jamais abraçaria pelo pavor que sempre tive de dilacerar alguém, ainda que fosse apenas para causar-lhe o bem — do que, propriamente, de juiz...

Em relação a esta terceira edição do livro da Dra. Patricia Peck, porém, não se aplicam tão amargas considerações. Em primeiro lugar, porque o sucesso das edições anteriores já falam por si e dispensam todo e qualquer tipo de apresentação da autora, já sobejamente conhecida entre os estudiosos do tema... Em segundo lugar, porque o *Direito na sociedade da informação* ou *Direito virtual* ou *Direito do espaço virtual* ou *Direito da Internet* ou, ainda, como a autora prefere designar, *Direito digital*, entre tantas designações possíveis¹, constitui um novo e extraordinário campo de reflexão para o jurista contemporâneo, dele exigindo a *sofisticação teórica*, tão justa e oportunamente reivindicada pelo eminente Prof. Ricardo Luís Lorenzetti², uma das maiores autoridades do nosso continente sobre a matéria, conforme se vê do seguinte trecho, o qual, muito amiúde, aprez-me reproduzir³:

1. *Cyberlaw* ou *Cyberspace Law*, nos Estados Unidos; *Cyberdroit*, na França; *Diritto dell'internet*, na Itália; *Derecho del espacio virtual*, na Espanha e em outros países de língua castelhana.

2. Cf. *Tratado de los contratos*, Rubinzal-Culzoni Editores, Santa Fé, Argentina, abril de 2000, Tomo III, Capítulo LXVII, *Informática, Cyberlaw, E-Commerce*, p. 833 e, posteriormente, republicado em *Direito & Internet — Aspectos jurídicos relevantes*, obra coletiva, Newton De Lucca e Adalberto Simão Filho (coordenadores), 2. ed., São Paulo: Quartier Latin, 2005, p. 465 e s.

3. Não só em palestras proferidas sobre o tema como em vários artigos a respeito do mesmo, sendo de destacar-se, como um dos últimos deles, o prefácio à obra da Prof^a Cláudia Lima Marques, intitulada *Confiança no comércio eletrônico e a proteção do consumidor (um estudo dos negócios jurídicos de consumo no comércio eletrônico)*, São Paulo: Revista dos Tribunais, 2004.

“O surgimento da era digital tem suscitado a necessidade de repensar importantes aspectos relativos à organização social, à democracia, à tecnologia, à privacidade, à liberdade e observa-se que muitos enfoques não apresentam a sofisticação teórica que semelhantes problemas requerem; esterilizam-se obnubilados pela retórica, pela ideologia e pela ingenuidade”.

Já tive a ocasião de assinalar, em oportunidade anterior⁴, o paralelismo que se pode traçar entre o papel desempenhado pelas estradas de ferro, no decorrer do século XIX — sem dúvida, as principais responsáveis pelo extraordinário desenvolvimento dos países que as fizeram construir em seus territórios —, e aquele que será exercido pelas *estradas da comunicação digital*. Deverão ser estas, doravante, as grandes geradoras de ganhos, de ordem qualitativa e quantitativa, para as economias nacionais que se beneficiarão da dinamização da cadeia de fornecedores e da expressiva diminuição de custos e das margens de estoque.

Ninguém porá em dúvida que a transição que vivemos é evidente. Assim como a Revolução Industrial modificou, no passado, as feições do mundo moderno, a ainda incipiente Revolução *Digital* já está transformando as faces do mundo pós-moderno. A diferença entre uma e outra — se é que se tenha segurança, hoje, para tentar estabelecer uma relação ontológica entre ambas — situa-se na velocidade surpreendentemente maior com que as referidas transformações irão ocorrer durante a segunda.

Enquanto na sociedade industrializada era a quantidade de trabalho investida nos produtos e serviços que servia de paradigma de valor, na sociedade *digitalizada* será a quantidade de informação e conhecimento que tais produtos e serviços conseguirem agregar que determinará a formação do paradigma.

O palco onde ocorrerá o *topos* dessa agregação é o chamado *ciberespaço*⁵,

4. *Direito do consumidor — Teoria geral da relação jurídica de consumo*, 2. ed., São Paulo: Quartier Latin, 2008, p. 440 e 441.

5. Contra uma expressiva maioria, continuo a preferir a expressão *espaço cibernético* a *ciberespaço*, conforme já me manifestara em Títulos e contratos eletrônicos — o advento da Informática e seu impacto no mundo jurídico, in *Internet e direito — Aspectos jurídicos relevantes*, obra coletiva, São Paulo: Edipro, 2000, p. 28, nota de rodapé n. 18. Sem embargo da ampla discussão possível no plano filológico, o fato é que a palavra *ciberespaço* não era encontrada, até bem pouco tempo, em nossos dicionários, constituindo-se num evidente barbarismo. Já em inglês, *cyber* possui sentido específico. Dizer-se que *ciber* poderia ser usado pelo fato de já existir, como prefixo de *Cibernética*, não aproveita em nada, porquanto esta última palavra deriva do grego, *Kybernetes*, ou *piloto*, a mesma palavra grega da qual tenha sido derivada, talvez, a palavra *governador*. Diz Norbert Wiener (*cibernética e sociedade, o uso humano de seres humanos*, tradução de José Paulo Paes, São Paulo: Cultrix, s/d, p. 15) ter descoberto “casualmente, mais tarde, que a palavra já havia sido usada por Ampère com referência à ciência política e que fora inserida em outro contexto

no qual ocorre, segundo o filósofo Pierre Lévy, uma “globalização de significados”, *in verbis*:

“O ciberespaço dissolve a pragmática da comunicação que, desde a invenção da escrita, havia conjugado o universal e a totalidade. Ele nos reconduz, de fato, à situação anterior à escrita — mas numa outra escala e numa outra órbita —, na medida em que a interconexão e o dinamismo em tempo real das memórias em rede faz com que o mesmo contexto, o imenso hipertexto vivo, seja compartilhado pelos integrantes da comunicação⁶”.

Por ocasião da segunda edição do presente livro, tive a oportunidade de assinalar que a autora era não apenas uma escritora de vanguarda, mas, principalmente, de uma vanguarda séria, que sabe distinguir, com a prudência de que falavam os romanos, inspirada na frônesis grega, o que deve ser tido por bom e por justo.

Verifico, com satisfação ainda maior, o caráter *in fieri* desta obra da Dra. Patricia, pois os acréscimos havidos nesta 3ª edição revelam a preocupação da autora em fazer com que a dinâmica inerente ao mundo virtual não empalideça a atualidade de sua pesquisa jurídica.

Assim é que novos temas como os da espionagem eletrônica; da Gestão Eletrônica de Documentos (GED), monitoramento da marca na Internet; aspectos legais das eleições na Internet (ePolítica); seguro de risco eletrônico; VoIP; Web 2.0 e boas práticas para *Service Level Agreement* (SLA) — todos consistentes no que se poderia chamar *de vanguarda* — foram oportunamente agregados à edição que ora se dá à estampa, igualmente atualizada com a indispensável referência a julgados de 2007 e 2008, à legislação vigente e a Projetos de Lei em andamento, além de nova doutrina a respeito da matéria.

Não tenho dúvidas em afirmar, portanto, que a Dra. Patricia Peck Pinheiro fornece a todos os que militam na área da advocacia empresarial — e,

por um cientista polonês; ambos os usos datavam dos primórdios do século XIX.” Não obstante esta minha preferência, porém, estar-me-ei utilizando, no decorrer do trabalho e em eventuais traduções, da palavra *ciberespaço*.

6. Cf. A globalização de significados, *Folha de S. Paulo*, Caderno Mais, edição de 7 de dezembro de 1997. O mesmo Pierre Lévy, em outro artigo (Cultura traz intelectuais de olho no futuro, *O Estado de São Paulo*, edição de 24 de dezembro de 2000, Caderno telejornal, p. T6), destaca que a comunicação do saber é a chave do futuro, sendo necessária uma democracia conveniente à sociedade da *comunicação rápida* — segundo sua expressão — “que nos faça ver a vitalidade da invenção e do pensamento coletivo”.

em especial, no âmbito mais específico do Direito *Digital* — um utilíssimo instrumento de trabalho.

São Paulo, junho de 2008.

Newton De Lucca

Professor do programa de educação continuada e especialização em Direito GVlaw.

Mestre, Doutor, Livre-Docente e Adjunto pela Faculdade de Direito da Universidade de São Paulo, onde leciona nos Cursos de Graduação e Pós-Graduação.

Coordenador Acadêmico e Científico do Mestrado Europeu em Direito Empresarial da Escola Paulista de Direito em convênio com a Universidade Lusófona de Lisboa.

Professor do Corpo Permanente da Pós-Graduação Stricto Sensu da Faculdade Autônoma de Direito — FADISP.

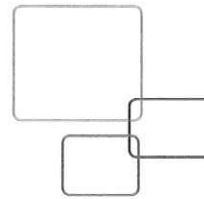
Desembargador Federal do TRF da 3ª Região.

Membro da Academia Paulista de Magistrados.

Membro da Academia Paulista de Direito.

Presidente da Comissão de Proteção ao Consumidor no âmbito do comércio eletrônico do Ministério da Justiça.

Diretor-Presidente da Escola dos Magistrados da Justiça Federal da 3ª Região.



Prefácio à 2ª Edição

Recebemos com muita satisfação o convite formulado pela autora para que prefaciássemos a 2ª edição deste livro. Tal entusiasmo deve-se a motivação dupla. Em primeiro lugar, a Dra. Patricia tem sido permanente, incansável e eficaz colaboradora do Gabinete de Segurança Institucional da Presidência da República (GSI) em nossos constantes esforços para a implantação da Política de Segurança da Informação na Administração Pública Federal. Essa política foi definida pelo Decreto n. 3.505, de 13 de junho de 2000, e, para implantá-la, o decreto em seu art. 6º criou o Comitê Gestor da Segurança da Informação com a atribuição de assessorar o GSI. Esse comitê é atualmente composto por 16 ministérios e representa o braço político dessa implantação. Entretanto, logo ficou patente que carecíamos de um órgão operacional com dedicação exclusiva que pudesse tratar no âmbito de nosso gabinete e no cotidiano as diversas atividades concernentes a essa complexa tarefa. Criamos então no interior de nossa estrutura orgânica, há mais de um ano, o Departamento de Segurança da Informação e Comunicações. É especialmente com esse departamento e outras organizações parceiras que a autora tem colaborado nas ações de conscientização e capacitação dos membros do governo nos assuntos relativos à Segurança da Informação e Comunicações.

A segunda razão de nosso contentamento deve-se à natureza do presente livro, que, além de ser uma revisão e alargamento do anterior, acrescenta diversos capítulos novos que tangenciam mais veementemente nossas atividades. Enquanto em seu livro anterior a Dra. Patricia deu maior ênfase às reflexões

sobre a Sociedade Digital e o papel do Direito na regulação das novas modalidades dos relacionamentos pessoais e jurídicos, no atual ela detalha os aspectos legais da Segurança da Informação, abordando institutos como o da Legítima Defesa na Internet, a necessidade da Conscientização dos Usuários, certas tendências como a de uso de uma Identidade Digital Obrigatória, a questão da guarda adequada da Prova Eletrônica e as boas práticas para terceirização em TI, entre outros. Assim, além das brilhantes palestras e aulas que a autora costuma ministrar em nossos eventos, agora contaremos com o presente livro como um repositório mais detalhado de suas ideias.

No cotidiano da atual era da informação que estamos vivenciando, assistimos estarecidos às constantes modificações nas bases estruturais de nossa sociedade, que não só afetam, mas também tendem a homogeneizar, sem que nos apercebamos, as próprias culturas e tradições que por tanto tempo cultivamos. Abrangem desde inovações tecnológicas que nos envolvem e fascinam no nível individual às poderosas ferramentas voltadas para a automação de processos de desenvolvimento, fabricação e gestão, utilizadas por pequenas e grandes empresas ou mesmo Estados nacionais. Com a crescente disseminação da banda larga até os últimos confins do Planeta, pessoas, grupos ou mesmo comunidades inteiras localizadas em quaisquer regiões da Terra podem trabalhar, discutir e conversar como se estivessem frente a frente. Hoje as interfaces são as minúsculas câmeras de TV e as telas dos monitores, a cada dia com maior definição, com imagens cada vez mais nítidas. Num amanhã não muito distante estaremos — a parcela da humanidade que estiver incluída digitalmente — imersos numa realidade virtual holográfica, acompanhados de seres reais, existentes em outro lugar do Planeta, ou mesmo hipotéticos, criados por algum programador alhures. Os germens dessas coisas já existem nos *videogames* de hoje. O desenvolvimento vertiginoso das tecnologias de informação e comunicações não está apenas transformando a nossa realidade. Está criando uma nova realidade, um novo universo onde as dimensões do espaço são suprimidas e as leis da física são substituídas pelas leis da computabilidade. Estamos a meio caminho do “Matrix”.

É nesse contexto complexo e composto de eventos ocorrendo em dois tipos de realidade que o Direito Digital se deve inserir. É aí que a filosofia do direito deve buscar as bases de seu estabelecimento, os critérios de validação de suas leis. Muito apropriadamente, em seu livro anterior a autora acrescenta o elemento Tempo à fórmula tridimensional e tradicional do direito: fato, valor e norma. Deveras, as normas devem ser estabelecidas entre os fatos e os valores, entre a realidade e a moral, entre o que é e o que deveria ser. Assim, se por um lado a moral permanece estável, por outro os fatos estão se modificando com tal rapidez que foi necessária a introdução no Direito Digital da dimensão Tempo.

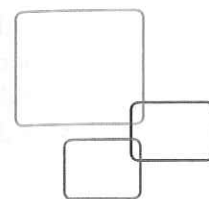
Considerando que poucos advogados têm plena habilitação em Direito Digital, o presente livro pode servir como referência não apenas para as grades curriculares dos cursos de direito, mas também para que os demais tomem conhecimento das sutilezas, particularidades e minúcias da moderna advocacia.

Jorge Armando Felix

Ministro de Estado

Chefe do Gabinete de Segurança Institucional

da Presidência da República



Prefácio à 1ª Edição

O Direito reflete, evidentemente, as mudanças culturais e comportamentais da sociedade. A teoria tridimensional o considera como fato, valor e norma, o que expressa bem a exigência da evolução da ciência jurídica em consonância com a realidade social. Dessa capacidade de adequação decorre, aliás, a própria segurança do ordenamento jurídico, projetado por meio de normas válidas e eficazes.

Na dinâmica da era de informação atual não é fácil para o legislador acompanhar as novas formas de conduta, de relações. Talvez escape à natureza humana a possibilidade de prever as múltiplas transformações tecnológicas que se sucedem num mundo denso, caracterizado, sobretudo, pela velocidade da transmissão da informação agora, também, digital. A mesma dificuldade encontra o aplicador do Direito diante da ausência de norma regulamentadora do assunto, técnico e aparentemente dissociado do cotidiano.

Com o objetivo de abordar a matéria e apontar soluções para as questões jurídicas surgidas, nesse novo campo, a Dra. Patricia Peck lança o presente livro, *Direito Digital*, cuja ideia central “é mostrar uma nova visão sobre o papel do profissional do Direito na sociedade digital, onde ele deve deixar de ser um burocrata para se tornar um estrategista...”. Os temas tratados na publicação estão colocados de modo a mostrar a necessidade da “reengenharia do universo jurídico”. A partir da Introdução, analisa a autora, em capítulos coordenados, os seguintes temas: “Da invenção do rádio à convergência de mídias”; “Conceitos que constituem a estrutura fundamental do pensamento jurídico”; “Rumo

à sociedade digital”; “Sociedade digital”; “A evolução do Direito”, culminando com a análise do “Direito Digital”; seus institutos jurídicos; e mais a “Responsabilidade civil e dano moral no Direito Digital”; “Ética e educação digital”; “Contratos”; “Arbitragem”; “O novo profissional do Direito”; “A gestão do risco eletrônico”; “Minutas” e Glossário sobre a matéria.

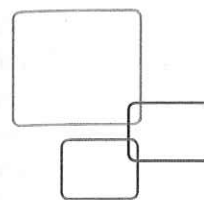
Apresenta a Dra. Patricia, como se observa da transcrição supramencionada, um alentado estudo sobre o Direito Digital, que responde aos presentes desafios e consiste “na evolução do Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas”.

Aponta a autora, ainda, as características do Direito Digital: a celeridade, o dinamismo, a autorregulamentação, poucas leis, base legal na prática costumeira, o uso da analogia e solução por arbitragem. Considera, aliás, a mediação e a arbitragem como vias únicas sustentáveis dentro da dinâmica imposta pela velocidade das mudanças para a solução dos conflitos, invocando a Lei n. 9.307, de 1996, que se origina de Projeto, de minha autoria, apresentado na qualidade de Senador da República, e permite a inclusão de cláusulas arbitrais em contratos (art. 4º, § 4º). O tempo, por conseguinte, é fundamental para o deslinde das questões, tanto que a Dra. Patricia Peck acrescenta que o Direito Digital é a aplicação da fórmula tridimensional do Direito, adicionada de um quarto elemento, o tempo.

O livro *Direito Digital*, que tenho a satisfação de prefaciá-lo, reveste-se, portanto, de importância não somente pelo seu conteúdo fundamentado, e pelas teses defendidas com inteligência, clareza e objetividade pela autora, mas, também, pela atualidade do tema na época globalizada e, de certa forma, digital em que vivemos.

Marco Maciel

*Vice-Presidente da República
(Governo FHC — 2002)*



Nota da Autora — O Direito Digital em Transformação

A realidade mudou. O tempo real invadiu o dia a dia de trabalho, com tudo para ontem, excesso de informação e carência de conhecimento. É preciso saber tanto de tantas coisas que temos a sensação de estar desatualizados a cada clique. As novas regras de conduta, nascidas da tendência crescente de proteção da privacidade, segurança da informação e governança corporativa, trouxeram novas exigências para o profissional do Direito atual.

Atravessamos um momento de ruptura, na qual se desenham os novos valores que devem ser protegidos e ensinados. O que é ético e legal dentro da sociedade digital? Como usar adequadamente as ferramentas tecnológicas de trabalho? O que significa soberania? Até onde vai a privacidade? Quais as consequências do monitoramento dentro da empresa? O que é o direito de autor, considerando os modelos atuais de produção colaborativa e terceirizada? O *e-mail* é correspondência? Os dados eletrônicos como “logs” são prova? Como entender o fenômeno da identidade do indivíduo em ambientes eletrônicos, com o uso de certificação digital ou biométrica? É errado enviar *spam*? É crime criar um vírus? E a fraude eletrônica? Todas essas questões merecem resposta — e quem for capaz de trazer soluções para elas tem a oportunidade de se diferenciar. Este é o papel exigido e cobrado dos operadores do Direito, quer sejam magistrados, advogados, peritos, procuradores, promotores.

A Revolução da Informação, plantada em 1957, com a criação do primeiro *mainframe*, marcou o começo da digitalização da sociedade. Hoje, vivemos uma interdependência completa, globalizada, interativa e em rede. Uma simples

página gratuita na Internet já nasce global, com responsabilidades e obrigações dentro de um cenário complexo de normas. Somos reflexo não apenas de nosso conhecimento, do “penso, logo existo”, mas de nossa expressão, do “comunico-me, logo existo”: *blogs*, páginas pessoais, comunidades, fóruns, *chats*, *messengers*. E como fica a questão da prova da identidade, tão importante em situações de responsabilidade profissional, civil e criminal, com estes diversos “eus” em jogo?

Quando a sociedade muda, o direito também deve mudar. O Direito Digital consiste numa evolução do próprio direito, abrangendo todos os princípios fundamentais vigentes e introduzindo novos institutos e elementos para o pensamento jurídico em todas as áreas: direito constitucional, civil, autoral, comercial, contratual, econômico, financeiro, tributário, penal, internacional etc. Questões complexas, como proteção de marcas e domínios e uso de serviços de governo eletrônico, e simples, como uma compra em loja virtual, exigem nova postura do intérprete do Direito. Já não basta haver um conjunto de leis. É preciso estabelecer uma interpretação dinâmica, interagir no ambiente em que está a manifestação de vontade, como num *videogame* em que se deve entender a regra no próprio jogo.

É este pensamento que norteia o princípio cada vez mais disseminado do uso da Autorregulamentação e da prática da Mediação e Arbitragem na solução dos conflitos. Por isso cresce a demanda por políticas, códigos de conduta, *disclaimers*, entre outras peças que devem estar inseridas nos *sites*, na intranet da empresa, na extranet, nos contratos com cláusulas que solicitam ciência e provas guardadas no formato original, que agora é o eletrônico.

O próprio modelo de contrato passa a receber novas cláusulas, que tratam sobre responsabilidade por atualização de versão, segurança da informação, propriedade de conteúdos e bancos de dados, nível de garantia de serviço, entre outras. Não é admissível, hoje, a redação de um documento jurídico sem que haja uma introdução com um glossário, que explique o significado de termos como, por exemplo, Internet. Pois, afinal, o que é Internet? Já não é apenas uma rede mundial de computadores, pois há celulares, *palms*, geladeiras, carros, casas conectadas. Sem a definição adequada dos conceitos, estamos sujeitos à subjetividade na interpretação, e portanto a riscos legais.

Estamos quebrando paradigmas. As relações atuais e a manifestação de vontade que as legitima já se tornaram eletrônicas. O arquivo original não é mais o papel, mas o dado, que deve ser guardado de modo adequado à preservação de sua autenticidade, integridade e acessibilidade, para que sirva como prova legal. Nessa nova realidade, a versão impressa é cópia, e as testemunhas são as máquinas.

Para refletir sobre quais os impactos jurídicos e sociais dessa nova realidade, cito Alain, em *História de meus pensamentos*, que diz: “Toda consciência é de ordem moral, pois sempre opõe o que deveria ser ao que é”.

É muito importante interpretar este conceito com o de liberdade, constante na Declaração dos Direitos do Homem e do Cidadão: “A liberdade consiste em poder fazer tudo o que não prejudica o outro, de modo que os únicos limites do exercício dos direitos naturais de cada homem são aqueles que garantem aos outros membros da sociedade o gozo desses mesmos direitos, e esses limites só podem ser determinados pela lei”.

Logo, no decorrer de nossas vidas, fomos educados nos conceitos de “certo” e “errado”, dentro dos valores sociais estabelecidos e das normas vigentes. No entanto, a tecnologia trouxe novos comportamentos e condutas que precisam de orientação e treinamento para poderem estar também alinhados com os mesmos preceitos que já aprendemos, garantindo assim a segurança jurídica das relações.

Apesar de já ser rotina para todos nós executar ações como enviar um *e-mail*, falar ao celular, acessar o Internet Banking, ler uma notícia *online*, escrever um conteúdo em um *Blog*, participar de um *Chat*, fazer uma Compra *online*, registrar um Domínio, pedir ajuda a outro colega via *instant Messenger*, tirar uma foto digital, preencher um cadastro em um *Hotsite* de Promoção *Online*, para muitos não são claros os limites e as responsabilidades envolvidas nessas atividades. Não faz parte do senso comum, por exemplo, que o *e-mail* corporativo é o papel timbrado digital da empresa, que todo conteúdo escrito na Internet é de responsabilidade de seu autor, que enviar um boato eletrônico pode gerar responsabilidade civil e criminal, que registrar uma palavra-chave com nome de um concorrente é crime de concorrência desleal, que em Comunidades *Online* nunca se pode falar de questões da empresa protegidas por sigilo profissional, que furtar o *mailing* da empresa é tão condenável quanto furtar um bem físico.

Ou seja, desde pequenos ouvimos que não devemos deixar a porta de casa aberta (que é o mesmo que dizer para não deixar o computador aberto e logado sem usuário), que não devemos falar com estranhos (que é o mesmo que abrir um *e-mail* de remetente desconhecido ou um anexo suspeito), que não devemos dirigir sem cinto de segurança (que é o mesmo que usar o computador sem antivírus e *firewall*), que não devemos caminhar sozinhos por ruas desertas e desconhecidas, principalmente à noite (que é o mesmo que acessar *sites* não seguros), que só devemos assinar depois de ler as letras miúdas dos contratos (que é o mesmo que ler atentamente as Políticas Eletrônicas e *Disclaimers*, antes de dar o clique no “sim”), que não devemos deixar nossos docu-

mentos soltos, e se os perdemos, devemos fazer um Boletim de Ocorrência (que é o mesmo que não passar sua senha ou sua assinatura digital para outro usar), entre outros.

Assim como no mundo real, na Internet o crime espreita a cada esquina, a cada clique. Corremos riscos sem perceber. Principalmente porque somos desatentos, negligentes, omissos. Não está clara a regra do jogo, e, além disso, ainda banalizamos as condutas. Tudo é apenas uma “palavrinha”, apenas um “e-mailzinho”, apenas um “arquivinho”, apenas um “gifizinho”. Só que isso pode significar quebra de sigilo, infração a direito autoral, crime de difamação, de falsa identidade, de fraude, podendo gerar responsabilidades civis, criminais, trabalhistas, tanto para a pessoa como para a empresa. Que atire o primeiro *mouse* quem nunca infringiu nenhuma regra eletrônica.

Há leis suficientes. Estamos abastecidos tanto pela legislação nacional como pela internacional, com destaque para o novo Código Civil, que ampliou a responsabilidade do gestor em seus arts. 1.011 e 1.016, além da Constituição Federal de 1988, do Código Penal, do Código de Defesa do Consumidor, da CLT e regulamentações (CVM, BACEN, Sox, Basileia II etc.), Lei de Direitos Autorais, que é de 1996, a Lei de *Software*, que é de 1988. Se pensarmos bem, muita coisa mudou nos últimos dezessete anos, desde a forma como as pessoas se relacionam com o uso da tecnologia até às próprias leis.

Como dar segurança jurídica e da informação garantindo o mínimo de identidade e privacidade? Nenhuma estratégia de Segurança da Informação terá êxito se não incorporar os quatro níveis de controle social do Direito: 1) nível ético, que são os valores; 2) nível cultural, que é a educação; 3) nível tecnológico, que são os processos; e 4) nível legal, que são as normas.

Mais do que trazer novas questões jurídicas, o Direito Digital exige de todos um papel de estrategista. É preciso pensar antes para preparar o terreno, para saber quais são as testemunhas. Além disso, exige um permanente monitoramento: o direito está baseado em ferramentas de controle de comportamentos. Já não há barreiras territoriais nem temporais, e isso trouxe ampliação da responsabilidade, que está cada vez mais solidária e objetiva.

Pois estamos falando do ser humano, não de máquinas. Segundo Nietzsche, “a linguagem é a expressão adequada de todas as realidades”. Ou seja, se não usarmos a linguagem adequada, estaremos deturpando a realidade. E vale ainda mencionar Wittgenstein: “Os limites de minha linguagem significam os limites de meu próprio mundo”. Logo, enquanto falarmos de tecnologia, estamos falando para um universo limitado de indivíduos. Precisamos traduzir isso dentro dos princípios gerais, dos costumes já estabelecidos, para gerar elemen-

tos de familiaridade que permitam o aprendizado e a prática. Só com informação e conscientização podemos realmente combater as vulnerabilidades.

O Direito Digital deve ser estudado não só para fins profissionais, mas para a formação dos cidadãos desta nova era, a fim de poder continuar a exercer a liberdade individual sem prejuízo da vida coletiva em uma sociedade totalmente conectada, em que a ação de um pode gerar efeitos e consequências em cascata para todos. É preciso aprender estas novas regras sob pena de ficarmos obsoletos.

Dra. Patricia Peck Pinheiro

Há pouco mais de quarenta anos, a Internet não passava de um projeto, o termo “globalização” não havia sido cunhado e a transmissão de dados por fibra óptica não existia. Informação era um item caro, pouco acessível e centralizado. O cotidiano do mundo jurídico resumia-se a papéis, burocracia e prazos. Com as mudanças ocorridas desde então, ingressamos na era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigmas. Essa nova era traz transformações em vários segmentos da sociedade — não apenas transformações tecnológicas, mas mudanças de conceitos, métodos de trabalho e estruturas. O Direito também é influenciado por essa nova realidade. A dinâmica da era da informação exige uma mudança mais profunda na própria forma como o Direito é exercido e pensado em sua prática cotidiana.

É importante compreender que vivemos um momento único, tanto no aspecto tecnológico como no econômico e social. O profissional de qualquer área, em especial o do Direito, tem a obrigação de estar em sintonia com as transformações que ocorrem na sociedade. Sabemos que o nascimento da Internet é um dos grandes fatores responsáveis por esse momento, mas o que é fundamental, antes de tudo, é entender que esses avanços não são fruto de uma realidade fria, exclusivamente tecnológica, dissociada do mundo cotidiano.

A Internet é mais que um simples meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de indivíduos. Indivíduos com letra maiúscula, porque estão inseridos em um conceito mais amplo, que abrange uma indivi-

dualização não só de pessoas físicas como também de empresas, instituições e governos. A Internet elimina definitivamente o conceito de corporação unidimensional, impessoal e massificada. Isso significa profunda mudança na forma como o Direito deve encarar as relações entre esses Indivíduos.

É diante de tal conjuntura que entendemos oportuna esta reflexão sobre a evolução do Direito para atender à sociedade digital. Nossa abordagem irá mostrar os princípios que deram origem ao Direito, sua aplicação na realidade prática atual, as lacunas que devem ainda ser preenchidas. Nossa proposta é desenvolver o tema de Direito Digital trazendo soluções que possam atender às lacunas do Direito hoje e sobreviver ao futuro que está por vir.

Dois fatos históricos foram essenciais para o amadurecimento de várias questões jurídicas que serão apresentadas no âmbito da sociedade brasileira: 1990, ano da criação do primeiro Código Brasileiro de Defesa do Consumidor, e 1995, quando o Ministério das Comunicações publicou a Norma 004¹, que regula o uso de meios de rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à Internet, marcando o nascimento comercial do sistema no País. Esses dois fatos colocam o Brasil em plenas condições de acompanhar as transformações mundiais no mesmo passo que as nações de ponta. Significam que a sociedade brasileira está plenamente inserida numa rede global de Indivíduos e, ao mesmo tempo, que estes adquirem capacidade de resposta cada vez maior, jurídica e cultural, às suas demandas.

A criação de uma consciência do consumidor e a entrada da Internet nas residências foram essenciais para que pudéssemos construir um pensamento jurídico sustentável, com base em padrões de conduta vivenciados na experiência de problemas práticos e de soluções que já vêm sendo aplicadas, algumas boas e outras a serem ainda aperfeiçoadas.

A proposta deste livro é provocar discussão, pois a discussão leva ao descobrimento da verdade, ao entendimento, sendo este um princípio de inteligência. Vamos estudar o que está além da tecnologia, do mundo digital e da informação, visto que o Direito é a soma de tudo isso, é a magnífica harmonia entre linguagem e comportamento. A ideia é mostrar o novo papel do profissional do Direito na sociedade digital, em que ele deve deixar de ser um mero burocrata para se tornar um estrategista, comunicando-se com as demais áreas dessa sociedade. Os temas estão estruturados de modo bem objetivo para podermos enxergar melhor esta reengenharia do universo jurídico.

Pretendemos mostrar que o Direito já não é resultado do pensamento solitário de um jurista, mas sim uma solução prática de planejamento e estratégia que só pode ser feita em equipe, num contato direto com as demandas e a própria evolução da sociedade. Essa solução deve ser capaz de adaptar-se a transformações cada vez mais rápidas e mudar também quando necessário.

Toda mudança tecnológica é uma mudança social, comportamental, portanto jurídica. Após realizar várias palestras, percebi que já era o momento de disponibilizar esse conhecimento adquirido em casos práticos, acertos, erros, dúvidas, curiosidade, criatividade, audácia, inovação. Estes termos não nos são ensinados nas Faculdades de Direito e hoje são os diferenciais competitivos para um profissional que não só estuda as leis, como estuda o Homem, o comportamento e o equilíbrio das forças que regem a sociedade.

O Direito não é nem deve ser complexo. Deve ser simples e com alto grau de compreensão das relações sociais, estas sim complexas. Quando a sociedade muda, deve o Direito também mudar, evoluir. Convido todos a um novo olhar, um novo pensamento, a perceber as transformações que o Direito está vivendo e aceitar o desafio de começar uma nova era, a era do Direito Digital. A ideia por trás desse convite é demarcar um novo território, abordando as mudanças profundas que ocorrem na sociedade contemporânea para, a partir disso, dotar os estudantes e profissionais do Direito dos instrumentos necessários para atuar neste novo mercado. Por isso, peço licença a meus colegas para dar soluções e não apenas apresentar questões jurídicas.

1. Aprovada pela Portaria n. 148, de 31 de maio de 1995.

Da Invenção do Rádio à Convergência de Mídias: Os Reflexos Comportamentais das Mudanças Tecnológicas

Alvin Tofler destacou, nos anos 70, a emergência de uma sociedade da informação. A sociedade da informação seria regida por dois relógios: um analógico e um digital. O relógio analógico seria aquele cuja agenda segue um tempo físico, vinte e quatro horas por dia, sete dias por semana. O relógio digital seria aquele cuja agenda segue um tempo virtual, que extrapola os limites das horas do dia, acumulando uma série de ações que devem ser realizadas simultaneamente. Sendo assim, a sociedade da informação exige que, cada vez mais, seus participantes executem mais tarefas, acessem mais informações, rompendo os limites de fusos horários e distâncias físicas; ações que devem ser executadas num tempo paralelo, ou seja, digital.

Para Tofler, a velocidade de tomada de decisão dentro de uma organização seria o instrumento de sua própria sobrevivência. Hoje, vivemos esta realidade. A agilidade imposta às empresas da economia digital exige um pensamento jurídico capaz de ultrapassar a barreira do tempo exigido pelas repartições públicas, pelos órgãos de registro, pelo Poder Judiciário. Se a fórmula jurídica estiver errada, mesmo que se possa corrigi-la, o custo do tempo pode ser fatal.

A sociedade humana vive em constante mudança: mudamos da pedra talhada ao papel, da pena com tinta ao tipógrafo, do código Morse à localização por *Global Positioning System* (GPS), da carta ao *e-mail*, do telegrama à videoconferência. Se a velocidade com que as informações circulam hoje cresce cada vez mais, a velocidade com que os meios pelos quais essa informação circula e evolui também é espantosa.

A sociedade da informação citada por Tofler tem suas origens na expansão dos veículos de comunicação surgidos na primeira metade do século XX, agrupados genericamente sob o nome de meios de comunicação de massa. Essa definição é um reflexo do momento histórico em que tais veículos cresceram e, hoje, pode ser contestada pelo nascimento de uma sociedade convergente que tem como principal característica a diversidade.

Segundo Tofler, a evolução da humanidade poderia ser dividida em três ondas. A primeira delas teve início quando a espécie humana deixou o nomadismo e passou a cultivar a terra. Essa Era Agrícola tinha por base a propriedade da terra como instrumento de riqueza e poder. A Segunda Onda tem início com a Revolução Industrial, em que a riqueza passa a ser uma combinação de propriedade, trabalho e capital. Seu ápice se dá com a Segunda Guerra Mundial, em que o modelo de produção em massa mostra sua face mais aterrador: a morte em grande escala, causada pelo poderio industrial das nações envolvidas.

Como em toda transição, a chegada da Terceira Onda, a Era da Informação, começou a dar seus primeiros sinais ainda antes do apogeu da Segunda Onda, com a invenção dos grandes veículos de comunicação, como o telefone, o cinema, o rádio e a TV, num período de cinquenta anos entre o final do século XIX e início do século XX. Esses veículos, nos quais trafegam volumes crescentes de informação — a característica central da Terceira Onda —, conheceram sua expansão ainda a serviço do modelo de produção em grande escala, de massificação, centralização de poder e standardização ditado pela Era Industrial.

É o surgimento da tecnologia digital, culminando na criação da Internet, que permite a consolidação da Terceira Onda, pela inclusão de dois novos elementos: a velocidade, cada vez maior na transmissão de informações, e a origem descentralizada destas.

Segundo o canadense Marshall McLuhan, um dos mais importantes teóricos das comunicações, havia uma contraposição entre a sociedade fortemente baseada na palavra escrita, surgida com o advento da Imprensa, pela invenção de Gutemberg no século XV, e uma sociedade eminentemente visual, em que cinema e TV desempenham o papel principal. À linearidade da primeira McLuhan opõe o caráter dinâmico dos segundos e prega sua universalidade: cinema e TV seriam os responsáveis pelo surgimento de uma Aldeia Global, onde toda a humanidade estaria interligada. O problema é que a teoria de McLuhan foi elaborada na primeira metade do século XX e trazia, implicitamente, uma questão terrível: os veículos definidos por ele como pontas de lança de uma nova era têm caráter essencialmente massificante.

McLuhan já previa uma “aldeia global”, com um número cada vez maior de pessoas conectadas a uma única rede. Mas o que temos hoje, além de um universo conectado, é uma grande diversidade, causada pela individualização e pelo que Tofler chama de *overchoice* — um mundo em que as possibilidades de escolha são infinitas. Esse cenário transcende a previsão do teórico canadense. Ou seja, se para McLuhan o meio era a mensagem, hoje, a mensagem é o meio. Isso determina uma forma distinta de enxergar a própria aplicação do Direito.

Para Nicholas Negroponte, há um terceiro elemento que caracteriza a informação na Era Digital: seu caráter de riqueza inesgotável. No modelo industrial, cada bem de consumo produzido é indivisível e tem um fim único. Na indústria da informação, os bens¹ podem ser infinitamente duplicados por quem quer que seja: o exemplo básico é um *software*² — no momento em que um consumidor faz um *download* de um *software*, ele não o está tirando de uma fábrica ou uma loja e levando para sua casa: está simplesmente copiando o produto. E esse produto pode ser copiado tantas vezes quantas forem necessárias. Esta evolução das mídias traz desafios sucessivos para o universo jurídico.

Os desafios jurídicos do Direito Digital incluem a quebra de paradigmas, a descentralização, a dificuldade em definir limites territoriais e físicos, a velocidade com que as decisões devem ser tomadas e a crescente capacidade de resposta dos indivíduos. A Internet gera uma infinidade de nações virtuais — pessoas, empresas e instituições de várias partes do mundo unidas por interesses os mais variados.

O grande desafio do Direito é enfrentar essa contradição entre globalização e individualização, que é a grande característica de nossa era — uma era de transição, em que convivem conceitos aparentemente tão díspares. Na nova ordem mundial, não é possível receitar um mesmo remédio para toda a economia. No caso brasileiro, esse desafio é ampliado por vivermos em uma sociedade que, durante tanto tempo, esteve sob regimes autoritários e, em sua cultura jurídica, guarda ainda muitos resquícios desse autoritarismo. Para enfrentar uma realidade tão difusa e complexa, é imprescindível que os profissionais do

1. O Código Civil de 2002, em seu art. 83, III, iguala os direitos pessoais de caráter patrimonial e respectivas ações a bens móveis, para efeitos legais.

2. A Lei n. 9.609/98 — Lei de Programa de Computador —, que substituiu a Lei n. 7.646/87 — Lei do *Software*, em seu art. 1º, parágrafo único, assim o define: “Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados”.

Direito revejam sua forma de atuação, aplicando os princípios fundamentais e desenvolvendo novas soluções para atender às demandas futuras.

3

Os Conceitos que Constituem a Estrutura Fundamental do Pensamento Jurídico

Onde há normas jurídicas a conduta humana torna-se, em alguns sentidos, obrigatória e não optativa. O Estado de Direito tem como princípio fundamental a liberdade do homem, sendo seus estatutos concebidos para adequar, dentro do ordenamento jurídico-social, os conceitos basilares que limitam essa liberdade, conferindo ao cidadão um direito subjetivo e irrenunciável.

O Direito é uma pretensão garantida pela existência de um poder superior capaz de obrigar, de impor suas decisões. Sendo assim, caracteriza-se por ser um sentido de valor que está em permanente tensão com a realidade social. Por ser essencialmente comportamental — e porque o comportamento humano é, em sua essência, mutável e evolutivo —, há uma instabilidade inerente ao próprio Direito.

Para Hans Kelsen, o comportamento é normatizado pelo Direito, que lhe confere um atributo de valor e uma sanção, sem a qual não há como garantir a eficácia da norma. Dessa forma, a base da obrigação jurídica e moral de nossa sociedade está sustentada num sistema que envolve um conjunto de abstenções e concessões mútuas, chamado de sistema coercitivo.

A meta do ordenamento jurídico é ser uma organização centralizada do poder que teria como vantagens a adaptabilidade diante das mudanças, o que garantiria o seu grau de certeza e eficácia na sociedade. Há, então, a participação interativa da realidade no momento de concepção da norma, havendo uma adaptação valorativa desta ao contexto social.

A positivação do Direito nasceu de uma necessidade de limitar o poder dos governantes por meio da criação de normas impessoais, concebidas para efetivar a racionalização do poder. São normas voltadas para a estabilidade da sociedade, o que não impede haja a instabilidade intrínseca ao Direito, resultante da tensão permanente dos valores com a própria realidade.

Compete ao Sistema Legislativo fazer o filtro de todas as valorações e expectativas de comportamento da sociedade, mediante processos decisórios, para que elas possam adquirir validade jurídica. A capacidade da norma de refletir a realidade social determina o grau de eficácia jurídica de um ordenamento. Eficaz é aquilo que é capaz de efetivamente produzir efeitos, ou seja, o conceito de eficácia envolve aceitação e obediência.

Norma eficaz é aquela que é observada e cumprida pelos diversos grupos sociais. Implica o chamado “hábito geral de obediência”, sendo a garantia de cumprimento da norma. Assim, a pressão social é que daria origem à obrigação vinculada pela norma que preestabeleceria os critérios de conduta a serem seguidos. A adaptação à mudança é uma exigência de sobrevivência da própria norma. Hoje, a problemática está na velocidade que a mudança vem adquirindo e na dificuldade do sistema jurídico em incorporá-la.

Um breve exemplo: Lawrence Lessig¹, um dos maiores especialistas mundiais em Direito Digital, afirma que os códigos de *software* podem ser comparados a leis, ou seja, o código-fonte dos *softwares*, assim como as leis, tem o efeito de controlar o comportamento de maneiras específicas. Por exemplo, você sabe que, quando quer usar os serviços de determinado provedor de acesso, precisa fornecer sua senha. É requisito imposto a você pelo código do Provedor de Acesso. Portanto, seria possível escrever uma lei dizendo que você precisa identificar-se adequadamente. Mas isso seria menos eficiente. Ambos são estruturas projetadas para controlar o comportamento. São diferentes de uma maneira importante: é mais fácil violar uma lei do que violar um código-fonte. Então certamente seria uma mudança se algumas leis sagradas fossem implementadas com tecnologia de *software*. Tal raciocínio mostra como as normas e a maneira clássica de pensar o Direito podem ser transformadas pelo surgimento de uma nova realidade social.

A capacidade de adaptação do Direito determina a própria segurança do ordenamento, no sentido de estabilidade do sistema jurídico por meio da atuação legítima do poder capaz de produzir normas válidas e eficazes. A segu-

rança das expectativas é vital para a sociedade, sendo hoje um dos maiores fatores impulsionadores para a elaboração de novas leis que normatizem as questões virtuais, principalmente a Internet.

Este sentimento de que se fazendo leis a sociedade se sente mais segura termina por provocar verdadeiras distorções jurídicas, uma vez que, como vimos, nem toda norma válida é eficaz. O Direito é responsável pelo equilíbrio da relação comportamento-poder, que só pode ser feita com a adequada interpretação da realidade social, criando normas que garantam a segurança das expectativas mediante sua eficácia e aceitabilidade, que compreendam e incorporem a mudança por meio de uma estrutura flexível que possa sustentá-la no tempo. Esta transformação nos leva ao Direito Digital.

1. Para mais detalhes, visite o site: <<http://www.lessig.org>>.

Antes de nos aprofundarmos no conceito de Direito Digital, é importante entender outro conceito: o de Sociedade Convergente. Para isso, vamos traçar breve histórico da evolução tecnológica da qual essa sociedade é resultado.

A informática nasceu da ideia de beneficiar e auxiliar o homem nos trabalhos do cotidiano e naqueles feitos repetitivamente. Tem-se por definição mais comum que a informática é a ciência que estuda o tratamento automático e racional da informação¹. Entre as funções da informática há o desenvolvimento de novas máquinas, a criação de novos métodos de trabalho, a construção de aplicações automáticas e a melhoria dos métodos e aplicações existentes. O elemento físico que permite o tratamento de dados e o alcance de informação é o computador².

A necessidade de instrumentos que auxiliassem o homem a processar informações, em apoio a suas funções mentais naturais, não é recente. Pode-se dizer que remonta aos antigos pastores que utilizavam pedras para contabilizar seu rebanho — seria esta a figura representativa dos primórdios do processamento de dados.

1. KANAAN, João Carlos. *Informática global*. 2. ed. São Paulo: Pioneira, 1998. p. 23-31.

2. O computador é uma máquina composta de elementos físicos do tipo eletrônico, capaz de realizar grande variedade de trabalhos com alta velocidade e precisão, desde que receba as instruções adequadas.

O primeiro engenho concebido com essa finalidade seria o ábaco. Utilizado por mercadores há mais de 2.000 anos e filho direto das necessidades dos mercantis, o ábaco faz-se com pedrinhas — *calculi* — que, ordenadas segundo a técnica desenvolvida pelos matemáticos de então, auxiliavam a elaboração de cálculos e tarefas de contabilidade que, de outra forma, tomariam muito tempo³.

No século XVII, o escocês John Napier cria o mecanismo que chamou de “ossos de Napier”, o qual, por permitir a execução de operações matemáticas mais complexas, desdobrar-se-ia nas até recentemente muito utilizadas réguas de cálculo.

O filósofo francês Blaise Pascal construiu em 1642 um engenho mecânico capaz de somar e subtrair números de oito algarismos. Também filósofo, o alemão Gottfried Leibniz constrói em 1677 sua máquina de calcular. Somente em 1830, porém, a tecnologia é industrializada e começam a ser fabricadas na Europa máquinas de calcular mecânicas.

Em 1834, o norte-americano Charles Babbage constrói complexa máquina capaz de executar uma sequência predeterminada de operações matemáticas. Embora nunca tivesse sido finalizada como desejava seu criador, a máquina e as próprias anotações de Babbage lançaram conceitos até hoje fundamentais na computação: a máquina que executa comandos predefinidos — o programa, a interface de entrada/saída e a memória dos cálculos realizados.

Em 1847, o matemático britânico George Boole idealiza em sua obra *The mathematical analysis of logic: being an essay towards a calculus of deductive reasoning* uma teoria que aproxima a lógica da matemática, por meio de operadores lógicos (E, OU e NÃO) e um sistema binário de numeração que se utiliza apenas dos algarismos 1 e 0. Tal teoria ficou posteriormente conhecida como Álgebra Booleana e viria a ser amplamente utilizada nos computadores, que ainda tardariam a surgir, pela facilidade em associar os operandos booleanos (1 e 0) a dois estados da corrente elétrica (ligado e desligado).

O norte-americano Herman Hollerith concebeu em 1890 uma máquina eletromecânica que lia uma série de dados gravados em cartões perfurados e fez com que o censo daquele ano nos Estados Unidos fosse processado em um terço do tempo do censo anterior. Hollerith mais tarde fundaria a empresa *Tabulating Machine Company*, que hoje é conhecida pelo nome de *International Business Machine* (IBM).

A utilização de máquinas calculadoras mecânicas e eletromecânicas proliferou no início do século XX. Nos anos 30, essas máquinas começaram a ser

construídas com relés eletromagnéticos, porém somente em 1946 estaria finalizado o engenho que claramente se reputaria um passo além das calculadoras. Seu nome era ENIAC — *Electric Numeric Integrator and Calculator* —, um computador baseado em circuitos eletrônicos. Operava com lógica binária, composto de 18.000 válvulas, e ocupava diversas salas da Universidade de Pensilvânia, onde foi concebido.

A ideia estava maturada e era viável. Em 1951 foi lançado o UNIVAC I, o primeiro computador a ser vendido comercialmente. Daí em diante a microeletrônica passa a balizar os avanços na área. O advento do transistor nos anos 60, substituindo a válvula, diminui o tamanho, o consumo de energia e aumenta a potência dos computadores. Ainda nos anos 70 surgem os circuitos integrados, que têm esse nome por reunirem grande número de transistores em uma única peça⁴.

Os anos 70 viram o advento do microprocessador, minúscula partícula de silício que centraliza o processamento em um computador e onde eram condensadas centenas de transistores, os elementos que faziam os computadores ocupar grandes espaços, consumir grande quantidade de energia e estar em constante manutenção. As centenas de transistores tornaram-se milhares, dezenas de milhares e, em nossa época, centenas de milhares, fazendo dos microcomputadores pessoais, que utilizamos em nossas casas e escritórios, engenhos com capacidade de processamento superior à das grandes universidades, laboratórios e empresas de trinta anos atrás.

Como podemos perceber, além do que ficou exposto acima, nas últimas quatro décadas vários fatos contribuíram para uma profunda mudança na realidade social. Em 1964, Gordon Moore cria a Lei de Moore e revoluciona a produção dos *chips*. O primeiro computador com *mouse* e interface gráfica é lançado pela Xerox, em 1981; já no ano seguinte, a Intel produz o primeiro computador pessoal 286. Tim Bernes Lee, físico inglês, inventa a linguagem HTML (*HyperText Markup Language* ou, em português, Linguagem de Marcação de Hipertexto), criando seu pequeno projeto de World Wide Web (WWW), em 1989; Marc Andreessen cria o *browser Mosaic*, que permite fácil navegação na Internet, em 1993. Em 1996, Steve Jobs lança o iMac. No mesmo ano, dois estudantes americanos, Larry Page e Sergey Brin, em um projeto de doutorado da Universidade Stanford, criam o maior *site* de buscas da internet, o “Google”. Em 1999, um ataque de hackers tira do ar *websites* como Yahoo

3. História do computador. In: *Enciclopédia Britânica*. 1998. CD-ROM.

4. WEBER, Kival; MELIM, Angela. *A sociedade da informação*. Rio de Janeiro: Ed. Rio, 1980. p. 67.

e Amazon, entre outros. Em 15 de janeiro de 2001 é criada a “Wikipedia”, a primeira enciclopédia *online* multilíngue livre colaborativa do mundo, que pode ser escrita por qualquer pessoa, de qualquer parte do globo, de forma voluntária. Em 23 de outubro de 2001, cerca de um mês depois dos atentados de 11 de setembro, é lançada pela Apple a primeira versão do iPod, de 5GB e tela monocromática, aparelho que revoluciona o mercado de música mundial ao permitir, segundo o seu criador Steve Jobs, o “armazenamento de até 1000 músicas em seu bolso”. Os exemplos são muitos.

Esses fatos são reflexo de um caminho rumo à chamada sociedade convergente que se vem desenvolvendo rapidamente desde a criação do telefone, considerada a primeira ferramenta de comunicação simultânea a revolucionar os comportamentos sociais. Na outra ponta deste movimento evolutivo, a Internet veio possibilitar não apenas o encurtamento das distâncias com maior eficiência de custos, mas, sobretudo, a multicomunicação, ou seja, transmissão de texto, voz e imagem. A multicomunicação, associada à capacidade de respostas cada vez mais ágeis, permite que a Internet se torne o mais novo veículo de comunicação a desafiar e transformar o modo como nos relacionamos.

A origem da internet remonta ao ápice da “guerra fria”, em meados dos anos 60, nos Estados Unidos, e foi pensada, originalmente, para fins militares.

Basicamente, tratava-se de um sistema de interligação de redes dos computadores militares norte-americanos, de forma descentralizada. À época, denominava-se “Arpanet”. Esse método revolucionário permitiria que, em caso de ataque inimigo a alguma de suas bases militares, as informações lá existentes não se perderiam, uma vez que não existia uma central de informações propriamente dita.

Posteriormente, esse sistema passou a ser usado para fins civis, inicialmente em algumas universidades americanas, sendo utilizado pelos professores e alunos como um canal de divulgação, troca e propagação de conhecimento acadêmico-científico. Esse ambiente menos controlado possibilitou o desenvolvimento da internet nos moldes os quais a conhecemos atualmente.

Entretanto, o grande marco dessa tecnologia se deu em 1987, quando foi convencionalizada a possibilidade de sua utilização para fins comerciais, passando-se a denominar, então, “Internet”.

Na década de 90, a Internet passou por um processo de expansão sem precedentes. Seu rápido crescimento deve-se a vários de seus recursos e facilidades de acesso e transmissão, que vão desde o correio eletrônico (*e-mail*) até

o acesso a banco de dados e informações disponíveis na World Wide Web (WWW), seu espaço multimídia.

Tecnicamente, a internet consiste na interligação de milhares de dispositivos do mundo inteiro, interconectados mediante protocolos (IP, abreviação de *Internet Protocol*). Ou seja, essa interligação é possível porque utiliza um mesmo padrão de transmissão de dados. A ligação é feita por meio de linhas telefônicas, fibra óptica, satélite, ondas de rádio ou infravermelho. A conexão do computador com a rede pode ser direta ou através de outro computador, conhecido como servidor. Este servidor pode ser próprio ou, no caso dos provedores de acesso, de terceiros. O usuário navega na internet por meio de um *browser*, programa usado para visualizar páginas disponíveis na rede, que interpreta as informações do *website* indicado, exibindo na tela do usuário textos, sons e imagens. São *browsers* o MS Internet Explorer, da Microsoft, o Netscape Navigator, da Netscape, Mozilla, da The Mozilla Organization com cooperação da Netscape, entre outros.

Os servidores e provedores de acesso utilizam a estrutura do serviço de telecomunicação existente (no caso brasileiro, o *backbone* da Embratel), para viabilizar o acesso, armazenamento, movimentação e recuperação de informações do usuário à rede. O endereço IP é dado ao computador que se conecta à rede, e os subendereços são dados aos computadores conectados com os provedores. A tradução dos endereços IP, numéricos, para os seus correspondentes em palavras faz-se pelo protocolo DNS — *Domain Name System*. As terminações do endereço são feitas de acordo com os TLDs — *Top Level Domains* —, o primeiro grupo de caracteres após o último ponto de nome de domínio propriamente dito. Exemplos são o “.com”, “.gov”, “.net”, “.org”, “.tv”. Outros TLDs indicam o país de origem do usuário. Os registros são feitos em órgãos especializados. No caso brasileiro, o atual responsável pelos registros é o Núcleo de Informação e Coordenação do Ponto BR (NIC.br)⁵, através do *website* <http://registro.br>, o qual ficou legitimado no que antes era de responsabilidade da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP)⁶.

A interligação física e a uniformização do sistema de transmissão de dados entre as redes, por meio dos protocolos, permitiu, portanto, que a inter-

5. Proposta aprovada na reunião realizada no dia 21 de outubro de 2005 pelo Comitê Gestor da Internet no Brasil (CGI.br), atendendo às atribuições que lhe confere o Decreto n. 4.829/2003. A Resolução CGI.br n. 001/2005 e a Resolução CGI.br n. 002/2005 e seu Anexo I, cada qual em seu inteiro teor, estão publicadas no endereço eletrônico do servidor *web* do CGI.br <<http://www.cgi.br>>.

6. Site: <<http://www.fapesp.br>>.

net conquistasse maior amplitude no globo. Hoje, a comunicação pode dar-se com ou sem intervenção humana — no último caso está, por exemplo, o *Electronic Data Interchange* (EDI), em que há sistemas aplicativos previamente programados que enviam e recebem as informações. Esses sistemas são fundamentais para entendermos que o surgimento de uma sociedade convergente plena não se trata de uma abstração futurista, mas de uma realidade concreta.

Da transmissão de pacotes de dados simples, evoluímos para a transmissão de áudio e vídeo, ou seja, conteúdo multimídia. Esse foi o segundo passo a caminho da convergência. Para a transmissão multimídia, passou-se a exigir equipamentos mais capazes e redes de maior velocidade ou com maior largura de banda. Assim, a velocidade dos recursos tecnológicos foi crescendo rapidamente, até chegar à Banda Larga (*broadband*), com conexões ADSL⁷, cabo e satélite. Estamos seguindo para um mundo de transmissões em tempo real, por meio de tecnologia *streaming*, uma evolução do conceito de videoconferência e a inserção de redes multimídias digitais que possibilitem interatividade, como a desenvolvida com linguagem MPEG4.

O movimento de convergência, no entanto, vai além, saltando do computador para os aparelhos de TV, telefones celulares, *palm-tops* e outros dispositivos multimídia. Passa a abranger toda uma comunidade móvel, sendo manifestada em sua plenitude quando alcançamos a interatividade. Calcula-se que, atualmente, um lar de classe média contenha aproximadamente 200 *chips*, incluindo todos os aparelhos eletrônicos existentes. Esse cálculo inclui fornos micro-ondas, aparelhos de fax, máquinas de lavar roupas, aparelhos de som e outros. A convergência será total no momento em que todos esses *chips* passarem a conversar entre si. Pense no dia em que sua geladeira terá a capacidade de constatar a iminência de um defeito qualquer, jogar essa informação numa rede interna em sua casa e, automaticamente, enviar um *e-mail* para a empresa de assistência técnica, que poderá consertar o defeito remotamente, pela rede, sem precisar ir até sua casa. Parece futurismo, mas esse tipo de tecnologia já existe, por exemplo, em equipamentos médicos de ponta, como aqueles utilizados para ressonância magnética.

A complexidade de tal sistema, do ponto de vista jurídico, está nas relações resultantes desta interação, principalmente as relações comerciais. Este ambiente de pessoas conectadas tornou-se extremamente propício para o comércio — aqui surge o conceito de *e-commerce*. A grande vitrina virtual passa a

atrair não apenas empresas, mas também profissionais liberais, *shopping centers*, consumidores, redes de ensino a distância, hospitais, laboratórios, bancos, corretoras e todo aquele interessado em obter uma informação, colocar um produto ou serviço à venda, ou simplesmente buscar entretenimento. Surgem as comunidades virtuais, os portais horizontais, os portais verticais, os *websites* institucionais, as *homepages* pessoais, os *blogs* e *fotologs*, os metamercados de consumidor-consumidor (C2C), empresa-consumidor (B2C), empresa-empresa (B2B), empresa-empresa-consumidor (B2B2C) — uma verdadeira rede de apatriados. Todas essas relações entre pessoas e empresas passam a exigir novas regras, princípios, regulamentos, assim como possibilitam a aplicação de antigos princípios que continuam tão atuais para o Direito como o eram em sua origem.

Qual o próximo passo? Não sabemos, mas é importante compreender todo o mecanismo de funcionamento das novas tecnologias de comunicação, entre elas a internet, bem como sua evolução no futuro cenário de convergência, uma vez que o Direito é resultado do conjunto comportamento e linguagem. Só com essa compreensão é que podemos fazer leis, aplicá-las e dar soluções ao caso concreto. É diante de toda esta velocidade de mudanças que nasce o Direito Digital.

7. ADSL — *Asymmetric Digital Subscriber Line* — é uma tecnologia em que, por meio de uma linha de telefone, é possível transmitir dados em alta velocidade.

O avanço tecnológico na comunicação sempre perseguiu o objetivo de criar uma Aldeia Global, permitindo que todas as pessoas do mundo pudessem ter acesso a um fato de modo simultâneo. Este é o princípio que orienta a criação de redes mundiais de telejornalismo, como a CNN, além de toda uma rede Broadcast Digital para transmissões ao vivo e em tempo real, de qualquer lugar do mundo. O mundo financeiro também persegue essa mesma facilidade de comunicação, investindo grandes somas na modernização dos equipamentos para permitir a criação de uma comunidade financeira mais dinâmica. Os chamados programas de *home-brokers* já são uma realidade. Seguindo a necessidade de corte de gastos e controles maiores sobre as filiais, as empresas passam a investir em redes de comunicação interna, conectando todas as suas operações mundiais. Nesse estágio, os executivos experimentam plenamente as facilidades da comunicação rápida, economizando papel, pulsos telefônicos, viagens e tempo.

Este contato no trabalho passa a provocar uma necessidade de expandir tais benefícios para os lares. Assim começa o movimento para instalar um computador em cada casa. A convergência sai da esteira econômico-corporativa e passa a levar a tecnologia para dentro dos lares, interligando uma rede de consumidores ávidos por informação, serviços e produtos. Essa convergência total possibilita novas economias para as empresas, principalmente de custos operacionais, logística, vendas e distribuição, além de instituir um canal de venda personalizada, com maior eficiência para a aplicação do princípio de estoque zero.

Já demonstramos a complexidade de um mundo em que todos estão conectados em uma única aldeia e, ao mesmo tempo, têm a possibilidade de agir, como nunca antes na história da humanidade, como indivíduos. Os mercados financeiros, como grandes precursores dessa era de convergência, foram os primeiros a sentir na pele as dificuldades desse universo. Se, por um lado, é muito bom estar conectado, por outro o comportamento irracional de mercado afeta a todos, onde quer que estejam, de maneira nunca antes experimentada. A aludida complexidade é agravada pelo fator tempo, pela velocidade crescente com que os efeitos dessa rede de relações são sentidos em toda a parte. Desde o início da Era Mercantilista, os efeitos de uma crise local podiam ser sentidos em todo o mundo. Por exemplo, uma crise entre ingleses e chineses causada pelo comércio do chá no século XIX acarretava consequências na economia de todo o mundo, mas os efeitos dessa crise demoravam meses para chegar em todas as partes do Planeta. Hoje, com a velocidade de transmissão de informações, tais efeitos são imediatos tanto em Londres como em São Paulo, no Cairo como em Sydney.

Esse exemplo macroeconômico serve como alerta sobre a complexidade que enfrentamos em todos os setores da sociedade. A questão fica mais clara se refletirmos sobre um dos aspectos centrais da sociedade convergente: a interatividade, ou seja, a possibilidade de participação humana em um nível de inter-relação global. Vários avanços técnicos permitem que mais e mais pessoas atuem num mundo interativo: o movimento do *software* livre, da internet grátis, do MP3, entre outros. A interatividade exige que as empresas virtuais estejam preparadas para atender seus consumidores a qualquer tempo e em qualquer lugar. No mundo virtual e interativo, uma empresa sediada em Little Rock, Arkansas, vive com a possibilidade — e o risco — de interagir rapidamente com um consumidor de, digamos, Mendoza, Argentina, numa realidade de impensável há pouquíssimo tempo. Uma pessoa no interior de Goiás pode comprar e vender ações de uma empresa sediada na China com capital aberto na Bolsa de Nova York, EUA.

Ter uma janela aberta para o mundo exige muito mais que apenas a seleção do público-alvo. Exige a criação de uma logística jurídica que reflita a diversidade cultural dos consumidores/clientes virtuais.

No aspecto do atendimento ao consumidor, por exemplo, parte das empresas inseridas na rede recorre à terceirização, contratando *contact-centers*¹

1. *Contact-centers/call-centers/telemarketing* são as designações para centrais de atendimento destinadas ao contato com consumidores ou *prospects*, de forma ativa (ligação feita a partir da

especializados para atender a demandas de usuários de diferentes culturas e países. No aspecto jurídico, é preciso que os profissionais do Direito também estejam preparados para criar essa logística, sabendo que a todo momento terão de lidar com diferentes normas, culturas e legislações.

A internet hoje tem mais de 800 mil *websites* e são criadas mais de mil *homepages* por dia. Estamos falando não apenas de uma comunidade virtual, mas de várias comunidades virtuais que se aglomeram em torno de objetivos comuns, várias tribos com participantes de vários pontos do Planeta, de diversas culturas, sujeitos cada um a princípios de valor e normas distintas.

A globalização da economia e da sociedade exige a globalização do pensamento jurídico, de modo a encontrar mecanismos de aplicação de normas que possam extrapolar os princípios da territorialidade, principalmente no tocante ao Direito Penal e ao Direito Comercial. Essa tendência de globalização do próprio Direito não é nova. O Direito Internacional Privado de algum modo já vem, por meio de Convenções² e Tratados Internacionais, tentando estabelecer critérios mais uniformes de análise jurídica entre os vários Estados nacionais. Para o Direito Digital, porém, a questão vai além: devem ser criados novos princípios de relacionamento, ou seja, diretrizes gerais sobre alguns requisitos básicos que deveriam ser atendidos por todos os usuários da rede. A resolução dessas questões já possibilitaria segurança maior nas relações virtuais. O que é diferente de se criarem normas específicas cuja aplicação e eficácia fariam muito limitadas no tempo e no espaço.

Outra consequência da sociedade convergente é o aumento da distância entre países desenvolvidos e em desenvolvimento, em razão do que se chama de analfabetismo digital — um problema político-social consistente em ter uma massa de trabalhadores não preparada para o uso das novas tecnologias. A preocupação não é apenas educacional: afeta a capacidade de aproveitamento de mão de obra, até mesmo de nível superior. O fenômeno de marginalização social se dá pela incapacidade dos indivíduos de conhecer e dominar as

empresa para o cliente) ou receptiva (do cliente a empresa), usando telefone ou outros canais de comunicação. O termo mais abrangente é *Contact Center*, que inclui o contato por *e-mail*, fax, *chat* e Voz sobre IP, por exemplo (Fonte: <<http://www.calltocall.com.br/glossario.asp>>).

2. Podemos citar: a) a “Lei Modelo da United Nations Commission on International Trade Law (Uncitral) para o comércio eletrônico com guia para aplicação”, produzido pela primeira vez em 1996, atualizado em 1998. Esse documento é referência mundial e todos os países devem fundamentar-se nele ao regulamentar o comércio eletrônico em seu território. Disponível na íntegra em <www.uncitral.org>; b) a “Cartilha sobre Comércio Eletrônico e Propriedade Intelectual”, publicada pela WIPO/OMPI (<<http://www.wipo.int>>), que aborda questões como jurisdição e legislação aplicável, entre outras, relativas ao comércio eletrônico.

novas tecnologias — não basta saber escrever, é preciso saber enviar um *e-mail*. Ao mesmo tempo que a Era Digital abre maiores possibilidades de inclusão, a exclusão torna-se mais cruel. Aqueles que não tiverem existência virtual dificilmente sobreviverão também no mundo real, e esse talvez seja um dos aspectos mais aterroadores dos novos tempos.

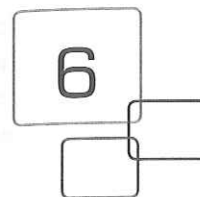
Globalmente, a presença da tecnologia passa a ser um novo fator de análise de subdesenvolvimento, ao mesmo tempo que equipara países que ainda não resolveram problemas primários, como saneamento básico e saúde, a outros em que essas questões já estão satisfatoriamente resolvidas. Por sermos todos visíveis, acessíveis, acabamos por concorrer pelas mesmas oportunidades de trabalho, negócios, produtos e ativos. Esse compartilhamento de territórios e entrada de novas peças no jogo mundial vai muito além, do ponto de vista jurídico, de operações de fusão e aquisição, alianças estratégicas, contratos de interconexão, entre outros. Significa uma rediscussão do conceito de soberania.

Atualmente, a maior parte dos *websites* da Internet está localizada nos Estados Unidos³. Porém, quem paga a maior parte da conta pelo uso dos *backbones* são os outros países, e o Brasil é um dos que vivem mais intensamente o problema. Isso porque, apesar de nossa febre pelo ciberespaço, a América Latina sofre a carência de “peering points” e vários de seus provedores ainda não fizeram a interconexão de suas redes. A autoestrada da informação está para a economia digital assim como a energia elétrica e as estradas estavam para a economia industrial. A disputa por seu controle já está sendo travada. Informação é poder, como foi um dia a propriedade da terra. Seguindo esta linha de raciocínio, quem estaria autorizado a colocar pedágios nessa autoestrada de informação? Quem deveria ser responsável por sua segurança e conservação?

3. Os Estados Unidos têm sido o administrador da Internet desde que a *web* foi criada como um projeto militar nos anos 60. Mas um grande número de países (como Brasil, China, Índia e, mais recentemente, a União Europeia) está contestando o controle norte-americano sobre a Internet. Eles argumentam que a Internet transformou-se em ferramenta global de comunicação e motor do crescimento econômico mundial e, por isso, não pode ser controlada pelos Estados Unidos. Em linguagem técnica, há uma batalha pela governança na Internet. Nos Estados Unidos estão localizados dez dos treze servidores-raiz (dois estão na Europa e um no Japão). Eles são o grande centro nevrálgico do acesso da *web*, pois sabem onde um computador tem de ir para achar o endereço de outra máquina. Em tese, os Estados Unidos têm o poder de tirar um país da Internet ou mesmo de decidir sobre o que é chamado de TLD (*top level domain*), como o .br. E não há nenhum organismo ao qual se possa reclamar das decisões ou vetos norte-americanos. Tal fato foi o tema principal durante a Cúpula Mundial da Sociedade da Informação (*World Summit on the Information Society*), que aconteceu em Túnis, na Tunísia, entre 16 e 18 de novembro de 2005 (Fonte: *IDG Now!*).

Se entendermos que a Internet é um lugar, então muitas questões do Direito devem ser redesenhadas, uma vez que o território ou jurisdição deveria ser a própria Internet. Se entendermos que a Internet é um meio, então voltamos a ter de resolver a questão da territorialidade para aplicação da norma, já havendo como referência a atuação do Direito Internacional.

Se a Internet é um meio, como é o rádio, a televisão, o fax, o telefone, então não há que falar em Direito de Internet, mas sim em um único Direito Digital cujo grande desafio é estar preparado para o desconhecido, seja aplicando antigas ou novas normas, mas com a capacidade de interpretar a realidade social e adequar a solução ao caso concreto na mesma velocidade das mudanças da sociedade.



A Evolução do Direito

Como defende o Dr. Samuel Huntington¹, o maior desafio da evolução humana é cultural. Podemos dizer o mesmo do Direito. Como instrumento de regulação de condutas, o Direito deve refletir a realidade da sociedade. Agora, quem adapta os legisladores e os aplicadores da lei à nova realidade social? Como fazer essa mudança cultural que está tão enraizada em todos nós? Estamos tão acostumados a trabalhar o tempo, as palavras, a paciência que para nós é muito difícil ser “trabalhados pelo tempo”, forçados a tomar decisões imediatas, mudar uma estratégia ou um posicionamento em questão de minutos, em virtude das mudanças no mercado, da concorrência, da variação das ações na bolsa, de um novo *business plan* etc. Também passamos a assumir maiores responsabilidades, sem muito tempo para pensar, refletir, fazer consultas. Isso quando há fontes para serem consultadas. Entretanto, adaptar-se a essa nova realidade significa dar continuidade à vocação histórica do Direito, que sempre seguiu as transformações ocorridas na estrutura da sociedade.

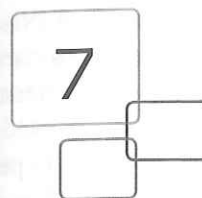
Na Era Agrícola, como vimos, o instrumento de poder era a terra, cujo domínio, no mundo ocidental, estava fortemente centralizado pela Igreja. Assim, o Direito era canônico, baseado em forte hierarquia, sob a justificativa de manter o controle e a paz social. Na Era Industrial, o instrumento de poder era o capital, que viabilizava os meios de produção. O domínio dele deveria ser do

1. *The Clash of Civilization*, Touchstone/Simon & Schuster, 1999.

Estado, que deveria proteger suas reservas contra ataques de outros Estados, sob a justificativa da soberania. O Direito, portanto, torna-se estatal e normativo, dentro de um sistema de comando e controles sobre os conceitos de territorialidade e ordenamento, em que a burocracia jurídica se transforma em mecanismo para a diminuição dos erros jurídicos e de monopólio da força.

Na Era Digital, o instrumento de poder é a informação, não só recebida mas refletida. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso à informação. Em vez de empresas, temos organizações moleculares, baseadas no Indivíduo. A mudança é constante e os avanços tecnológicos afetam diretamente as relações sociais. Sendo assim, o Direito Digital é, necessariamente, pragmático e costumeiro², baseado em estratégia jurídica e dinamismo.

2. O Direito Costumeiro, ou *Common Law*, é um Direito que utiliza o histórico de decisões de casos concretos como subsídio legal para uma ação judicial. Ou seja, ele cria um banco de dados de memória futura, tendo por referência os próprios costumes da sociedade. Este princípio deve reger o Direito Digital, de modo a imprimir um dinamismo que seja capaz de dar soluções rápidas aos conflitos.



Direito Digital

O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.).

Quem não lembra da resistência ao videocassete? Agora temos o Internet Banking, DVD, MP3, HDTV — *High Definition Television* —, TV Interativa, TV Digital, Banda Larga, WAP, VoIP. O que todas essas siglas significam para o mundo jurídico atual? Significa que são os novos profissionais do Direito os responsáveis por garantir o direito à privacidade, a proteção do direito autoral, do direito de imagem, da propriedade intelectual, dos *royalties*, da segurança da informação, dos acordos e parcerias estratégicas, dos processos contra *hackers* e muito mais. Para isso, o Direito Digital deve ser entendido e estudado de modo a criar novos instrumentos capazes de atender a esses anseios.

Da criação do *chip* ao lançamento do primeiro computador com interface gráfica para utilização doméstica se passaram quase vinte anos. Depois, as mudanças não pararam mais, culminando na convergência — nada mais que a integração de várias tecnologias criando uma rede única de comunicação inteligente e interativa que utiliza vários meios para transmitir uma mesma mensagem, em voz, dados ou imagem. É importante compreender que a ressaca tecnológica traz uma relação de dependência, atingindo pessoas, empresas,

governos e instituições. As relações comerciais migram para a Internet. Nesta janela, a possibilidade de visibilidade do mundo atual traz também os riscos inerentes à acessibilidade, tais como segurança da informação, concorrência desleal, plágio, sabotagem por *hacker*, entre outros. Assim, na mesma velocidade da evolução da rede, em virtude do relativo anonimato proporcionado pela Internet, crescem os crimes, as reclamações devido a infrações ao Código de Defesa do Consumidor, as infrações à propriedade intelectual, marcas e patentes, entre outras.

Historicamente, todos os veículos de comunicação que compõem a sociedade convergente passaram a ter relevância jurídica a partir do momento em que se tornaram instrumentos de comunicação de massa, pois a massificação do comportamento exige que a conduta passe a ser abordada pelo Direito, sob pena de criar insegurança no ordenamento jurídico e na sociedade. Foi assim com a imprensa, o telefone, o rádio, a televisão e o fax. Cada um deles trouxe para o mundo jurídico particularidades e desafios: a questão dos direitos autorais, a liberdade de imprensa, as restrições à programação por ofensa a valores ou moral, as encomendas por fax, as compras por telefone, a licença do jocoso para não cair na calúnia e na difamação, a proteção das fontes, os contratos dos anunciantes, os seguros de transmissão, entre outros. Com a Internet não há diferença: não existe um Direito da Internet, assim como não há um direito televisivo ou um direito radiofônico. Há peculiaridades do veículo que devem ser contempladas pelas várias áreas do Direito, mas não existe a necessidade da criação de um Direito específico.

O que propomos aqui, portanto, não é a criação de uma infinidade de leis próprias — como vimos, tal legislação seria limitada no tempo (vigência) e no espaço (territorialidade), dois conceitos que ganham outra dimensão em uma sociedade convergente. A proposta é que o Direito siga sua vocação de refletir as grandes mudanças culturais e comportamentais vividas pela sociedade. No Direito Digital prevalecem os princípios em relação às regras, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa. Por isso, a disciplina jurídica tende à autorregulamentação, pela qual o conjunto de regras é criado pelos próprios participantes diretos do assunto em questão com soluções práticas que atendem ao dinamismo que as relações de Direito Digital exigem.

No Direito Digital deve haver a publicação das “normas digitais” no formato de *disclaimers*, como já fazem os provedores, ou seja, estar publicada na página inicial a norma à qual se está submetido, sendo ela um princípio geral ou uma norma-padrão para determinada atuação. Desse modo, a publicidade das regras possibilita maior conhecimento do público e consequentemente

aumenta sua eficácia. Em nosso ordenamento jurídico ninguém pode alegar desconhecimento da lei¹, mas no caso do Direito Digital, em que a autorregulamentação deve prevalecer, faz-se necessário informar ao público os procedimentos e regras às quais está submetido, onde este ponto de contato com a norma se faz simultaneamente à situação de direito que ela deve proteger.

A velocidade das transformações é uma barreira à legislação sobre o assunto. Por isso qualquer lei que venha a tratar dos novos institutos jurídicos deve ser genérica o suficiente para sobreviver ao tempo e flexível para atender aos diversos formatos que podem surgir de um único assunto. Essa problemática legislativa, no entanto, não tem nada de novo para nós, uma vez que a obsolescência das leis sempre foi um fator de discussão em nosso meio. A exigência de processos mais céleres também sempre foi um anseio da sociedade, não sendo resultado apenas da conjuntura atual. Como exemplo de caminho mais rápido para a solução de conflitos, citamos a arbitragem, que existe nos Estados Unidos há mais de oitenta anos e já é muito praticada, principalmente em questões internacionais e comerciais.

Tomando por base todas essas referências, o Direito Digital traz a oportunidade de aplicar dentro de uma lógica jurídica uniforme uma série de princípios e soluções que já vinham sendo aplicados de modo difuso — princípios e soluções que estão na base do chamado Direito Costumeiro. Esta coesão de pensamento possibilita efetivamente alcançar resultados e preencher lacunas nunca antes resolvidas, tanto no âmbito real quanto no virtual, uma vez que é a manifestação de vontade humana em seus diversos formatos que une estes dois mundos no contexto jurídico. Logo, o Direito Digital estabelece um relacionamento entre o Direito Codificado e o Direito Costumeiro, aplicando os elementos que cada um tem de melhor para a solução das questões da Sociedade Digital.

No Direito Costumeiro, os elementos que estão a amparar o Direito Digital são: a generalidade, a uniformidade, a continuidade, a durabilidade e a notoriedade (ou publicidade). Para que esses elementos se ajustem ao Direito Digital, deve-se levar em conta o fator tempo, elemento de fundamental importância para um mundo em que transformações tecnológicas cada vez mais aceleradas ditam, de modo mais intenso, as transformações no próprio funcionamento da sociedade, determinando a importância de duas práticas jurídicas no Direito Digital: a analogia e a arbitragem.

1. Lei de Introdução ao Código Civil (Dec.-Lei n. 4.657/42), art. 3º: “Ninguém se escusa de cumprir a lei, alegando que não a conhece”.

Mesmo no caso brasileiro, em que o Direito Codificado é a base predominante, uma lei, ainda que não tenha sido revogada, perde validade se vários indivíduos deixam de comportar-se segundo ela por longo período de tempo. Ainda assim, o Direito Codificado limita as decisões jurídicas que muitas vezes têm de ser tomadas em pouquíssimo espaço de tempo, sendo, portanto, o Direito Costumey mais flexível.

A generalidade, uma de suas características centrais, determina que certo comportamento deva ser repetido um razoável número de vezes para evidenciar a existência de uma regra. É a base da jurisprudência, um fenômeno do Direito Costumey. No mundo digital, em muitos casos, não há tempo hábil para criar jurisprudência pela via tradicional dos Tribunais. Se a decisão envolve aspectos tecnológicos, cinco anos podem significar profundas mudanças na sociedade. Mesmo assim, a generalidade pode ser aplicada aqui, amparada por novos processos de pensamento do Direito como um todo: a norma deve ser genérica, aplicada no caso concreto pelo uso da analogia e com o recurso à arbitragem, em que o árbitro seja uma parte necessariamente atualizada com os processos de transformação em curso.

Sua aplicação imediata cumpre outra característica introduzida pelo Direito Costumey: a uniformidade. Se um consumidor tem uma decisão favorável contra um *site* que lhe vendeu algo e não colocou claramente um contato direto para reclamações em suas páginas, então é recomendável que todos os outros *sites* com problemas semelhantes procurem adequar-se a tal posicionamento, a fim de que não sofram as mesmas sanções. A morosidade causada pela não aplicação desses preceitos incentiva a elitização e o casuísmo, faz com que os mais fracos fiquem marginalizados perante a Justiça e não incentiva os consumidores a buscarem seus direitos. Por isso, a continuidade é importante, ou seja, essas decisões devem ser repetidas ininterruptamente, dentro de um princípio genérico e uniforme. A durabilidade é responsável pela criação da crença no uso desses elementos. A segurança do próprio ordenamento jurídico depende disso, assim como depende a competitividade das empresas quanto à necessidade de respostas rápidas para atuar num cenário de negócios cada vez mais globalizado e digital.

Para completar o raciocínio, é importante entender outra característica assumida pelo Direito Digital: a notoriedade. As decisões arbitrais devem sempre ser tornadas públicas, para que sirvam de referência aos casos seguintes e diminuam a obsolescência de decisões tomadas exclusivamente no âmbito do Judiciário — o que no Brasil significa tomar por base decisões de questões que começaram a ser discutidas há pelo menos cinco anos, um tempo que pode ser

fatal em uma época de velozes transformações como essa em que vivemos.

A prova é outra questão importante para a correta aplicação do Direito no mundo digital. Há hipóteses de inversão do ônus da prova devido, principalmente, aos princípios já protegidos pelo Código de Defesa do Consumidor. Um exemplo são as empresas que montam banco de dados de seus usuários na Internet: se o banco de dados for utilizado de forma incorreta ou ilegal, não cabe ao usuário que se sentiu lesado provar tal fato, mas à empresa acusada provar que não agiu dessa forma.

É importante ressaltar que a prova em meios eletrônicos é mais facilmente averiguada do que no mundo real, uma vez que há como rastrear quase tudo o que acontece. Esta memória de dados e acontecimentos entre máquinas, equipamentos, *softwares* permite que peritos especializados possam localizar, por exemplo, um *hacker* criminoso em qualquer parte do mundo, assim como identificar se uma compra foi feita em certo horário, por determinado IP e em determinado endereço.

No Direito Digital, em razão de muitas questões estarem previstas apenas em contratos, o princípio do *pacta sunt servanda*² também é fundamental. Assim, os contratos fazem a lei entre as partes, obrigando o cumprimento de seus termos, desde que estes estejam em conformidade com as regras e normas relacionadas³. Nesse ponto, destacamos a importância de todos os contratos que envolvam tecnologia possuírem cláusula de vigência, especialmente se pensarmos que a maioria dos *softwares* tem uma usabilidade muito curta, necessitando de constantes atualizações (*upgrades*) para continuar operando de forma adequada.

No caso de problemas específicos da Internet, o Direito Digital tem por base o princípio de que toda relação de protocolo hipertexto-multimídia, por ação humana ou por máquina, gera direitos, deveres, obrigações e responsabilidades. Logo, seja aplicando as leis atuais⁴, seja recorrendo ao mecanismo da analogia, dos costumes e dos princípios gerais de direito⁵, o Direito Digital tem o dever de regulamentar essas relações e intermediar os conflitos gerados por elas.

2. Princípio afirmativo de que os contratos existem para serem cumpridos, obrigando as partes nos limites da lei.

3. Código Civil, arts. 104 e 166, II.

4. Código Civil, arts. 107 e 112, que tratam da manifestação de vontade válida.

5. Lei de Introdução ao Código Civil (Decreto-Lei n. 4.657/42), art. 4º “Quando a lei for omissa, o juiz decidirá o caso de acordo com a analogia, os costumes e os princípios gerais de direito”.

Pelos motivos expostos acima, reiteramos que o Direito Digital não se limita à Internet, sendo a própria evolução do Direito onde a Internet é um novo recurso que deve ser juridicamente atendido, como todas as outras inovações que estejam por vir. Em tal realidade, o maior compromisso dos operadores do Direito Digital é evitar qualquer tipo de arbitrariedade. Por isso, a discussão dos projetos de lei sobre temas que envolvem informática, Internet, *e-commerce*, crimes virtuais deve ser feita com a sociedade civil, envolvendo empresas e organizações sociais, para não cometermos o erro de desmoralizar a lei, desacreditando o Direito.

As características do Direito Digital, portanto, são as seguintes: celeridade, dinamismo, autorregulamentação, poucas leis, base legal na prática costumeira, o uso da analogia e solução por arbitragem. Esses elementos o tornam muito semelhante à *Lex Mercatoria*⁶, uma vez que ela não está especificamente disposta em um único ordenamento, tem alcance global e se adapta às leis internas de cada país de acordo com as regras gerais que regem as relações comerciais e com os princípios universais do Direito como a boa-fé, *suum cuique tribuere*, *neminem laedere* e *honeste vivere*⁷.

Não devemos achar, portanto, que o Direito Digital é totalmente novo. Ao contrário, tem ele sua guarida na maioria dos princípios do Direito atual, além de aproveitar a maior parte da legislação em vigor. A mudança está na postura de quem a interpreta e faz sua aplicação. É errado, portanto, pensar que a tecnologia cria um grande buraco negro, no qual a sociedade fica à margem do Direito, uma vez que as leis em vigor são aplicáveis à matéria, desde que com sua devida interpretação. O Direito tem de partir do pressuposto de que já vivemos uma sociedade globalizada. Seu grande desafio é ter perfeita adequação em diferentes culturas, sendo necessário, por isso, criar flexibilidade de raciocínio, nunca as amarras de uma legislação codificada que pode ficar obsoleta rapidamente. Aqui voltamos para a questão dos Indivíduos, entendidos não só como pessoas, mas como empresas e instituições. Como sabemos, Direito é a somatória de comportamento e linguagem e, hoje, esses dois elementos estão mais flexíveis do que nunca, fato que demonstra que um direito rígido não deverá ter uma aplicação eficaz.

6. Conjunto de regras, princípios e costumes oriundos da prática comercial, sem vinculação a qualquer direito nacional.

7. Estas três expressões do latim traduzem três princípios basilares do Direito. *Suum cuique tribuere* significa "dar a cada um o que é seu; *neminem laedere* significa "a ninguém lesar; *honeste vivere* significa "viver honestamente".

7.1. O elemento tempo

A sociedade de direito institucionalizou o poder e deu ao ordenamento jurídico a tarefa de fazer a intermediação entre as atividades políticas e os valores morais, mediante uma fórmula tridimensional que consiste em Fato, Valor e Norma. O Direito Digital atua dentro destes conceitos, mas introduz um quarto elemento na equação: o Tempo. Torna-se, desse modo, um conjunto de estratégias que atendem a nossa sociedade digital e não mais apenas normas regulamentadoras.

Primeiramente, toda norma tem um elemento tempo determinado, que chamamos de vigência, ou seja, a duração dos efeitos de uma norma no ordenamento jurídico. No entanto, o elemento tempo no Direito Digital extrapola o conceito de vigência e abrange a capacidade de resposta jurídica a determinado fato. Ou seja, o conjunto "fato, valor e norma" necessita ter certa velocidade de resposta para que tenha validade dentro da sociedade digital. Esse tempo pode ter uma relação ativa, passiva ou reflexiva com o fato que ensejou sua aplicação, ou seja, com o caso concreto.

Consideramos como tempo ativo aquele em que a velocidade de resposta da norma pode implicar o próprio esvaziamento do direito subjetivo. Como exemplo, podemos citar o caso de uma empresa que necessita que um contrato de tecnologia seja cumprido e seja feito *upgrade* em seus equipamentos. Se ele não encontrar uma velocidade de aplicação, pode significar não só a obsolescência do que se está pleiteando como o seu esvaziamento. Foi o que aconteceu à época do *bug* do milênio⁸, em que a discussão de quem deveria ou não ser responsável pela modificação dos códigos não poderia ultrapassar a data da virada do ano, pois os efeitos seriam irremediáveis. Por sorte, nada de mais grave aconteceu, mas muitas empresas não conseguiram fazer valer seus contratos de tecnologia e arcaram com os custos sozinhas.

Consideramos tempo passivo aquele que é explorado principalmente pelos agentes delituosos, acreditando que a morosidade jurídica irá desencorajar a parte lesada a fazer valer seus direitos. Isso ocorre especialmente nas questões de direito do consumidor. Temos como exemplo a questão da entrega de uma mercadoria comprada na Internet, em que o consumidor deixa de fazer a reclamação por saber que, na maioria dos casos, a demora de decisão e todo o tempo

8. A respeito do *bug* do milênio podemos citar a Portaria n. 212, de 28 de maio de 1999, do Ministério da Justiça, sobre a responsabilidade dos desenvolvedores de *software* em reparar gratuitamente o *bug* do milênio.

a ser gasto são mais caros que o próprio valor da mercadoria. Então, uma série de empresas, cientes disso, não têm interesse na solução dos problemas com o consumidor, sendo a pressão social e o uso da imprensa os únicos mecanismos que conferem algum poder de coerção sobre elas, pelo medo de criar uma imagem negativa na marca e não pelo temor de um ordenamento jurídico eficaz.

Consideramos como tempo reflexivo aquele que opera de modo ativo e de modo passivo, simultaneamente, provocando efeitos em cadeia e prejudicando outros que se encontrem conectados no espaço virtual. Um exemplo disso é a questão dos crimes na Internet — a pedofilia⁹, a pirataria, a atuação de *hackers*, o jogo clandestino —, os quais, de algum modo, contaminam todos os que não necessariamente estariam praticando o delito.

A aplicação, portanto, da fórmula tridimensional do direito adicionada do elemento Tempo resulta do Direito Digital. Este quarto elemento é determinante para estabelecer obrigações e limites de responsabilidade entre as partes, quer seja no aspecto de contratos, serviços, direitos autorais, quer seja na proteção da própria credibilidade jurídica quanto à sua capacidade em dar solução a conflitos. Sendo assim, o advogado digital é um senhor do tempo, devendo saber manipular tal elemento em favor de seu cliente, pois um erro de estratégia jurídica pode ser fatal em uma sociedade em que a mudança é uma constante.

7.2. Territorialidade

Alguns outros princípios do Direito devem ser repensados dentro do escopo do Direito Digital, como o princípio da territorialidade. Onde fica a porta? Até onde um ordenamento jurídico tem alcance? O problema não está apenas no âmbito da Internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas¹⁰, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais.

9. Vale destacar a situação de fotos pornográficas na rede da empresa ou no computador que podem significar o crime descrito no art. 234 do Código Penal, o qual condena o seguinte ato em seu *caput*: “Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno: Pena — detenção, de 6 (seis) meses a 2 (dois) anos, ou multa”. Ainda pode ter uma circunstância agravante, quando cair, por exemplo, nos termos do art. 61, II, *b*: “contra criança, maior de 60 (sessenta) anos, enfermo ou mulher grávida”.

10. Lei de Introdução às Normas do Direito Brasileiro (Dec.-Lei n. 4.657/42), art. 9º, § 2º: “A obrigação resultante do contrato reputa-se constituída no lugar em que residir o proponente”. Código Civil, art. 435: “Reputar-se-á celebrado o contrato no lugar em que foi proposto”.

No mundo tradicional, a questão da demarcação do território sempre foi definida por dois aspectos: os recursos físicos que esse território contém e o raio de abrangência de determinada cultura. A sociedade digital rompe essas duas barreiras: o mundo virtual constrói um novo território, dificilmente demarcável, no qual a própria riqueza assume um caráter diferente, baseada na informação, que, como vimos, é inesgotável e pode ser duplicada infinitamente. A questão se complica se lembrarmos que, com a Internet, as diferentes culturas se comunicam o tempo todo. Não precisamos ir à Turquia para nos relacionarmos com alguém que vive no território geográfico da Turquia. Também, se pretendemos relacionar-nos culturalmente, por via do mundo virtual, com alguém desse território (aqui entendemos cultura no seu modo mais amplo, que inclui, por exemplo, a maneira como os Indivíduos encaram transações comerciais ou questões jurídicas), talvez seja preciso entendermos sua cultura de uma maneira mais profunda do que se nos deslocássemos fisicamente até lá. Em suma, no Direito Digital, temos de ter uma existência e um entendimento global.

A territorialidade é muito importante nesse aspecto. Que valores devemos proteger em relações de Indivíduos de origens distintas? O Direito sempre interfere nas relações humanas, seja em territórios distintos ou não, onde, de algum modo, deve-se proteger o que acontece nessas relações.

Para melhor esboçar a questão, vamos tomar como referência o Direito Internacional, pelo qual se estabeleceu que, para identificar a norma a ser aplicada, diante da extrapolação dos limites territoriais dos ordenamentos, deve-se averiguar a origem do ato e onde este tem ou teve seus efeitos, para que se possa aplicar o Direito do país que deu origem ou em que ocorreram os efeitos do ato.

Aqui entra um dilema importante, que não se aplica no mundo real: na Internet, muitas vezes não é possível reconhecer facilmente de onde o interlocutor está interagindo. Muitos *sites* têm terminação “.com”, sem o sufixo de país (por exemplo, sem o “.br” em seguida) o que teoricamente significa que estão localizados nos Estados Unidos. Só que vários deles apenas estão registrados nos Estados Unidos e não têm nenhuma existência física nesse país. Uma tendência mundial é assumir definitivamente o endereço eletrônico como localização da origem ou efeito do ato. Assim, se uma empresa brasileira registra um *site* como “.com”, em vez de “.com.br”, pode ter de se sujeitar às leis de diversos países no caso de questões jurídicas internacionais.

No caso da parte a ser protegida, um consenso é a busca da proteção ao lesado. Se, por exemplo, um consumidor chileno é lesado por um *site* brasileiro, serão aplicadas as leis de consumidor daquele país. Se esse *site* não quer res-

ponsabilizar-se por problemas que gere no Chile, deve deixar claro, de alguma forma, seu limite de atuação; deve informar quais os usuários que terá condições de atender e a que legislação está submetido¹¹, já que não necessariamente um *site* chileno tem empresa constituída no Chile, como o fato de um *site* brasileiro ter terminação “.com” não significa que tem empresa constituída nos Estados Unidos. Ter presença virtual representa a responsabilidade de poder ser acessado por Indivíduos de qualquer parte do mundo. Portanto, o princípio de proteção na sociedade da informação é justamente a informação.

Para a sociedade digital, não é mais um acidente geográfico, como um rio, montanha ou baía, que determina a atuação do Estado sobre seus Indivíduos e a responsabilidade pelas consequências dos atos destes. A convergência, seja por Internet, seja por outro meio, elimina a barreira geográfica e cria um ambiente de relacionamento virtual paralelo no qual todos estão sujeitos aos mesmos efeitos, ações e reações. É importante ressaltar, por último, que essa discussão sobre territorialidade não se esgota na necessidade de solucionar casos práticos, mas nos faz repensar o próprio conceito de soberania e, consequentemente, a concepção originária do próprio Estado de Direito.

Na questão da territorialidade, hoje se aplicam diversos princípios para determinar qual a lei aplicável ao caso. Há o princípio do endereço eletrônico, o do local em que a conduta se realizou ou exerceu seus efeitos, o do domicílio do consumidor, o da localidade do réu, o da eficácia na execução judicial.

Dependendo do caso, pode ser aplicado mais de um ordenamento. No Brasil, especificamente no tocante ao crime eletrônico, que hoje não tem barreiras físicas, ocorre de todo lugar, em todo lugar, causando vítimas, o Código Penal brasileiro alcança a grande maioria das situações, por meio da aplicação de seus arts. 5º e 6º¹².

11. Podemos facilmente verificar isso no portal Brasil Online (<www.bol.com.br>). O usuário deve aceitar os termos de um contrato em que são arrolados todos os direitos e obrigações de ambas as partes. Colhemos a seguinte cláusula para exemplificar o que acabamos de dizer:

“11. DISPOSIÇÕES GERAIS

11.1. Os termos dos serviços e o relacionamento entre as partes serão regidos pelas leis da República Federativa do Brasil, sem consideração a qualquer disposição sobre conflito de leis. Usuário e Brasil Online Ltda. concordam em submeter-se à competência única e exclusiva dos tribunais localizados no Brasil”.

12. Art. 5º do CP: “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional”.

Art. 6º do CP: “Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”.

7.3. Direito à informação e à liberdade de pensamento

A Sociedade Digital já não é uma sociedade de bens. É uma sociedade de serviços em que a posse da informação prevalece sobre a posse dos bens de produção. Essa característica faz com que a proteção do Direito à Informação seja um dos princípios basilares do Direito Digital, assim como a proteção de seu contradireito, ou seja, do Direito à não informação.

O direito à informação¹³ está desmembrado em três categorias, de acordo com o sujeito de direito: a) direito de informar, que é um direito ativo; b) o direito de ser informado, que é um direito passivo; c) o direito de não receber informação, que é um direito ativo e passivo.

A questão da informação assume maior relevância no Direito Digital em razão de seus desdobramentos comerciais e de responsabilidade civil¹⁴. O acesso à informação constitui o maior valor de uma sociedade democrática, e a massificação da Internet como serviço de informação e informatização possibilita um aumento de competitividade global de comunidades antes marginalizadas.

Ao mesmo tempo, o direito à não informação traz um limite ao direito de informar no qual o valor protegido é a privacidade do indivíduo. Mas como equilibrar essas relações sem que a intervenção do Estado para imposição de limites venha a ferir o direito de liberdade de pensamento¹⁵? Até onde um *e-mail* é adequado ou vira um *spam*, vira uma “invasão de privacidade”?

A solução desta questão se dá muito mais pelo comportamento do próprio mercado consumidor de informação do que pelo Estado ou pelo Direito. A livre

13. Está previsto na Constituição Federal de 1988, art. 5º, IV e IX, 220 e 221, IV; Recomendação n. 854 do Parlamento Europeu de 1979; Código de Honra das Nações Unidas de 1952.

14. Por exemplo, a publicação, em jornal, de fotografia, sem a autorização exigida pelas circunstâncias, constitui ofensa ao direito de imagem, não se confundindo com o direito de informação. Com esse entendimento, a 3ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo condenou o jornal *Diário Popular* (hoje *Diário de São Paulo*) a pagar indenização equivalente a 100 salários mínimos a Valdik Leite Trigueiro. Vítima de tentativa de assalto, Trigueiro teve sua foto, ao lado de um irmão, publicada no jornal. Em seguida à publicação da foto, o irmão da vítima foi assassinado (Processo n. 583.00.2000.640691-8, 1ª Vara Cível, TJSP).

15. Um episódio interessante que demonstra como pode ser indesejável a intervenção do Estado ao tentar restringir o conteúdo da Internet: em 1997, a Suprema Corte Americana julgou inconstitucional o CDA — *Community Decency Act* —, dando fim às aspirações do Congresso americano de controlar o conteúdo da Internet. Julgou a Suprema Corte que a lei infringia a Primeira Emenda da Constituição Americana, que garante a liberdade de expressão.

economia equilibra a relação de demanda e de oferta desde que haja transparência e competitividade, como acontece com as Bolsas e Mercados Financeiros.

A evolução da Internet do estágio quantitativo para o estágio qualitativo, como ocorre com todas as inovações tecnológicas, provoca uma transformação no direito à informação, pura e simplesmente, para o direito à informação de qualidade, ou seja, de informação autêntica com responsabilidade editorial pelo conteúdo. Essa mudança qualitativa torna o próprio consumidor capaz de determinar as regras e normas a serem obedecidas pelo mercado em um ambiente de competição, uma das formas de livre regulação que encontra na Lei da Oferta e da Procura sua solução.

É fundamental fazer a ressalva no tocante ao direito de liberdade de Expressão, que, com o advento dos mecanismos de comunicação e a sua disseminação, tem provocado certo conflito jurídico com outros direitos, como o da proteção da imagem e reputação do indivíduo. Devemos observar que a Constituição Federal de 1988 protegeu a liberdade de expressão em seu art. 5º, IV, mas determinou que seja com “responsabilidade”. Isso quer dizer que devemos interpretar a aplicação dela à luz do novo Código Civil, em seus arts. 186 e 187, que determina a responsabilidade por indenizar pelo dano causado, quer quando o ato ilícito tenha sido causado por ação ou omissão, quer quando é fruto do exercício legítimo de um direito no qual o indivíduo que o detém ultrapassou os limites da boa-fé e dos bons costumes.

Sendo assim, mesmo um consumidor que tem o direito de reclamação previsto no Código de Defesa do Consumidor pode vir a infringir a lei e ter de responder pelo dano causado por uma Comunidade *Online* criada cujo conteúdo seja difamatório.

Na era da Informação, o poder está nas mãos do indivíduo, mas precisa ser utilizado de modo ético e legal, sob pena de no exercício de alguns direitos estar-se infringindo outros, e isso não é tolerável em um ordenamento jurídico equilibrado. Nesse sentido, a tecnologia pode ser sim a solução para harmonizar as diversas forças sociais, ou então se tornar seu principal inimigo, causando estragos irreparáveis, como o cachorro que, em vez de proteger, morde a mão do próprio dono.

7.4. Privacidade e anonimato

O Direito Digital tem o desafio de equilibrar a difícil relação existente entre interesse comercial, privacidade, responsabilidade e anonimato, gerada pelos novos veículos de comunicação. Esta equação só pode ser equilibrada se

socialmente aceita e cobrada mediante procedimentos de vigilância e punibilidade que devem ser determinados pelo próprio Direito Digital. Se, por um lado, cresce a cada dia o número de empresas que disputam os consumidores da Internet e, conseqüentemente, a publicidade virtual, com preenchimento de formulários e cadastros, por outro lado, cresce também o nível de conscientização dos consumidores quanto à possibilidade de aplicação do atual Código do Consumidor, que trata da matéria de utilização de informações de consumidores para fins comerciais, trazendo uma série de penalidades para quem as pratica¹⁶.

Logo, não há lacuna jurídica no tocante à solução da privacidade¹⁷ na Internet. Há, sim, falta de entendimento quanto à aplicação de leis em vigor para questões relativamente novas, que exigem uma interpretação da norma e sua adequação ao caso concreto. Este é um princípio fundamental para a aplicação do Direito, o qual, conseqüentemente, deve ser adotado também no Direito Digital.

É evidente que o direito à privacidade constitui um limite natural ao direito à informação. No entanto, não há lesão a direito se houver consentimento, mesmo que implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida. Assim como há limites naturais ao direito à privacidade quando atinge interesses coletivos. Neste caso, a predominância do interesse coletivo sobre o particular requer verificação caso a caso.

Todo indivíduo deve ter direito a proteção de suas propriedades e de sua privacidade. Isso é indiscutível. No tocante à propriedade, há tanto bens tangíveis como bens intangíveis. Nesse sentido, suas informações, em última análise, são um ativo e, portanto, de sua propriedade, e merecem proteção. Mas será que a Sociedade Digital caminha nesse sentido, ou estamos indo para o lado oposto?

O grande paradigma não está no conceito ético ou mesmo filosófico se a privacidade deve ou não ser protegida. Claro que deve ser. Mas sim no modelo de negócios estabelecido, visto que a informação virou não apenas a riqueza do século XXI como também a moeda de pagamento.

16. Código de Defesa do Consumidor, arts. 22, 43, 44, 72 e 73.

17. A Constituição Federal do Brasil de 1988 resguarda a vida privada e a intimidade, assegurando sua inviolabilidade, conforme se lê no art. 5º, X: “*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*”.

Atualmente, uma pessoa pode comprar coisas, trocar, usar serviços gratuitos, tudo isso pagando com sua informação. Mas será que ela está pagando mais do que devia? Qual o limite? Cabe ao Estado delimitar algumas regras para evitar abusos, mas será que ele é capaz de fato de garantir seu cumprimento, que depende de infraestrutura e recursos de terceiros, estes entes privados?

Um valor tão importante quanto a privacidade é o livre-arbítrio. Por isso, a liberdade de contratar entre as partes, a livre-iniciativa é fundamental para o modelo democrático-capitalista. Não existe mais o “hipossuficiente” na forma como era enxergado e tratado há 30 anos. Ao contrário, a geração mais nova, que já nasce digital, sabe muito bem buscar e baixar conteúdos pagando por suas informações. Mas será que cabe ao Estado proteger este indivíduo dele mesmo, como foi feito quando determinou a proteção da vida e proibiu que uma pessoa pudesse tirar a própria vida?

Em princípio, já há proteções legais para a privacidade. No entanto, quando vamos para a prática, no dia a dia, mais operacional, não há nenhuma regra jurídica que imponha um limite máximo de tempo que uma empresa possa usar os dados de uma pessoa. Tampouco que determine quais são as formas legítimas de obtê-lo ou ainda que amarre em tipos de propósito de uso. Logo, se você se cadastrar em um serviço, gerará dois tipos de informação: a) a cadastral e b) a comportamental (de uso do serviço). As máquinas registram tudo. Seja a escolha de alimentos em um supermercado amarrado a um CPF de um plano de fidelidade e descontos, sejam as suas opiniões nas redes sociais (Facebook, Twitter, entre outros).

O que pode ser feito com esses dados? As empresas têm alterado suas políticas de privacidade para garantir maior propriedade dos dados para elas. Afinal, essa é a moeda de troca do uso do serviço. Mas como medir se é justo e proporcional? Será que a informação no seu perfil da rede social de que você tem como *hobby* jogar tênis permite que uma empresa use-a para abordá-lo? Seja para oferecer uma raquete de brinde ou vender uma assinatura de clube? Entendemos que, se a informação está pública e teve coleta legítima, e o uso está dentro de um propósito razoável, então sim, ela poderia. Mas você teria sempre o direito de pedir para parar de lhe contatar por este canal. Se seu número de telefone celular estiver disponível, a empresa pode lhe contatar, mas você pode pedir para não usar este meio de comunicação. Assim, fica razoável para ambas as partes.

Logo, um usuário tem o direito de não querer passar seus dados, bem como o de não querer que a empresa use sua informação; assim como a empresa tem o direito de não querer tê-lo como cliente. Se o usuário não concorda com os termos e políticas, não consegue seguir adiante. E, mesmo concor-

dando com tudo, se deixar de ser usuário do serviço, seus dados continuam com a empresa, em geral, para sempre, para qualquer propósito.

O assunto do momento das empresas da era digital, mais sustentável, cujas ações valem mais na Bolsa, é o “big data”. Ou seja, como gerar negócios com o grande banco de dados global que se tornou a web, principalmente com todas as informações publicadas pelas próprias pessoas na era pós-web 2.0. Quanto maior o potencial, maior o valor da própria empresa.

Por isso, qualquer lei sobre privacidade, proteção de dados sensíveis, para ser eficaz, tem que ser reflexo do modelo socioeconômico estabelecido e servi-lo. Se há discussões éticas sobre o modelo, devemos rever o próprio modelo antes de aplicar uma lei mais rígida que possa ter dois efeitos: a) não ser cumprida (dificuldade de impô-la inclusive para empresas fora do ordenamento jurídico de origem dos dados) e b) gerar como retaliação o apagão digital de protesto (as empresas retirarem os serviços do ar, o que lhes é de direito, visto que não terá mais como se pagar, pois não poderão usar os dados).

Em 2011 foi proposto o anteprojeto do Marco Civil da Internet, tornando-se o PL n. 2.126/2011, que dispõe sobre princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Isso é claro, pois, atualmente, com a existência de vários textos normativos, ainda não há uma lei específica que trate dos princípios voltados para o uso da Internet para viabilizar um melhor contato com o Direito. O Marco Civil será importante para a Sociedade da Informação porque será um sistema complementar às leis já existentes e preencherá lacunas legislativas. A privacidade é um dos princípios a serem discutidos: da mesma forma que existe a proteção constitucional, ela também é garantida na Internet, e é essa proteção de dados pela guarda de *logs* nos provedores que o anteprojeto discute, e uma das questões mais importantes para a sua aprovação.

A privacidade dos usuários, além de uma garantia, deve, também, ser protegida pelo Marco Civil da Internet, porque as informações dos usuários viraram moeda e são usadas como pagamento dos serviços que se dizem gratuitos, mas que retêm as informações dos indivíduos para sempre, utilizando-a para qualquer fim.

Quando se fala no Marco Civil da Internet, seu propósito inicial é garantir a privacidade de dados de consumidores e ter a guarda segura dos mesmos (igualando aos demais países do exterior), complementando o texto Constitucional, o Código de Defesa do Consumidor e o Código Civil. O texto apresentado ao Congresso Nacional está bem claro quanto à garantia de liberdade de expressão, todavia, deveria ter sido tratado melhor no que diz respeito à

vedação do anonimato prevista pela Constituição Federal. Além disso, privilegia o acesso à Internet a todo cidadão e deveria determinar a obrigação de o primeiro acesso ocorrer com educação sobre uso ético, seguro e legal da Internet, fazendo com que os usuários sejam conscientes, para orientá-los sobre o uso correto desta ferramenta, pois isso pode gerar abusos comuns à liberdade de expressão.

Um ponto preocupante do Marco Civil é quanto à identificação e guarda de logs de registro de acesso. Para o usuário chegar a um site de internet, deve passar pelo seu provedor de conexão. Essa conexão gera um registro, que contém seu número de IP com a data e hora do acesso. Depois, por meio da conexão, o usuário faz vários acessos em aplicações (podem ser serviços gratuitos de e-mail ou redes sociais) que precisam de cadastro. Esses acessos também geram registros, que guardam o número do IP, data e hora das ações do usuário. Por isso se faz necessário o registro das aplicações de dados de IP, data e hora utilizadas pelo usuário e deveria estar previsto no Marco Civil. Assim, entendemos que, ao solicitar o registro de conexão, é preciso identificá-lo para que haja a defesa digital. Para que a cadeia de identificação da prova de autoria funcione, ambos os registros devem ser obrigatórios, não somente o de conexão. O Marco Civil da Internet deve complementar e respeitar as leis em vigor.

A cultura da Internet no Brasil foi bastante difundida e debatida, sendo possível perceber que muitos dos registros de conexão e acesso a terem seu sigilo relativizado por ordem judicial se deram fora do âmbito processual penal. Por isso, não deve o Marco Civil retroceder nesse sentido, delimitando a aplicação da quebra do sigilo dos registros de conexão e acesso somente a processos de natureza criminal, pois há casos em que a competência é da Justiça Comum Cível ou Justiça Federal Trabalhista, as quais merecem o amparo desse recurso para solucionar determinadas lides.

Na questão do anonimato¹⁸, podemos ressaltar que ele é relativo, uma vez que a própria tecnologia nos permite rastrear o emissor, assim como rastreamos ligações telefônicas e sinais de rádio. A problemática do anonimato, portanto, deve-se ao comportamento de muitas empresas que não encaminham as queixas para investigação policial por medo de que a repercussão da matéria possa vir a prejudicar sua imagem no tocante à segurança. E é tal comportamento que faz com que não haja punição, o que contribui para o crescimento das práticas delituosas.

“Não existe almoço grátis.” Como já dizia a máxima popular, o modelo de negócios da internet está totalmente baseado no uso de informações como moeda de troca, de pagamento. Conteúdo é essencial na sociedade do conhecimento, e as pessoas comuns, os usuários digitais, se tornaram produtores e consumidores simultâneos de dados de forma frenética, em tempo real, globalizada. Mas será que deve haver um limite legal para estas relações ou negócios baseados em dados? Como um novo negócio na web pode usar as informações de seus clientes sem riscos legais?

Há uma expressão atual para retratar o modelo de riqueza da web que diz: se o serviço for gratuito, você não é o freguês, você é o produto! O Direito enfrenta sempre situações paradoxais, em que, por um lado, deve-se proteger a privacidade dos indivíduos, mas por outro, deve-se permitir a livre-iniciativa e a liberdade de contratar, em que uma pessoa pode escolher pagar algo com as suas informações.

No entanto, é condição ética e legal do negócio que essa regra esteja clara e transparente no momento da contratação. Por isso crescem as discussões sobre a criação de leis que tratem de proteção de dados sensíveis, que delimitem o uso das informações, e até mesmo que protejam mais a privacidade das pessoas na web. Mas isso é viável?

Há um elevado custo de infraestrutura para suportar tudo o que publicamos, acessamos e compartilhamos na internet. Vivemos uma realidade extremamente dependente de três insumos fundamentais, que possuem seus respectivos custos de produção: Energia, Telecomunicações e Tecnologia. Logo, como dar o adequado tratamento à economia dos dados, sem que isso gere um colapso do próprio modelo mercadológico estabelecido?

Esta questão não se detém apenas na privacidade, vai além, e alcança até a discussão no tocante à remuneração por direitos autorais e por direitos de imagem na web, em que aquele que gera audiência publicando conteúdos de terceiros é remunerado, mas não há necessariamente um repasse ao autor legítimo. E, nesse quesito, há grande risco implícito, de se estimular plágio e pirataria, o que torna o modelo não sustentável no longo prazo, já que, sem a proteção de quem cria, todos só vão querer copiar e em breve não haverá conteúdo de qualidade e com credibilidade nesta internet do “tudo grátis”.

Vivemos um momento crucial para reformatar o modelo, ajustá-lo e adaptá-lo com esse ganho de conhecimento dos últimos anos, mas sem repetir erros clássicos da indústria tradicional de conteúdo, em que o preço está amar-

18. Segundo a Constituição Federal do Brasil de 1988, art. 5º, IV: “é livre a manifestação do pensamento, sendo vedado o anonimato”.

rado a um modelo de distribuição concentrado e no qual o consumidor não adquire o conteúdo em si, mas apenas o suporte.

Quais seriam, então, as premissas necessárias para que a equação socioeconômico-jurídica consiga operar um crescimento sustentável e garantir inclusão digital, acesso à informação e a contínua oferta de informações relevantes na web? a) o conteúdo digital, depois de compartilhado, dificilmente consegue ser retirado totalmente da web; b) o mercado exige independência de suporte e liberdade de migração ou conversão de formato; c) aqueles que são os grandes beneficiados pelas audiências geradas pelos conteúdos de terceiros devem remunerar os autores (seja diretamente com uma porcentagem ou indiretamente pelo pagamento de uma taxa para uma entidade gestora de direitos autorais digitais globais); d) o pagamento por serviços gratuitos com uso de informações de indivíduos deve deixar claro para qual finalidade as informações serão usadas e por quanto tempo, afinal, não pode ser para sempre, como um cheque em branco, mesmo após o usuário já ter deixado de ser cliente do serviço.

Precisamos definir isso com urgência, seja por autorregulamentação de mercado, contratos, ou mesmo por meio de leis. Independentemente dos próximos passos, todo negócio que está na internet tem que ter uma política de privacidade atualizada, publicada, com conteúdo bem claro, para poder tomar proveito do mercado dos dados sem riscos legais. Fica a dica!

Já evoluímos muito na construção de uma sociedade na qual o privado e o público andam de mãos dadas para fechar a equação financeira. Não há espaço para utopias. Há, sim, necessidade de se delimitar algumas regras de conduta, que podem ocorrer até com autorregulamentação. E, antes de mais nada, há necessidade de transparência por parte das empresas, para que fique claro que dados serão usados, para qual finalidade, por quanto tempo.

Afinal, será que estamos dispostos a abrir mão de usar os serviços gratuitos, as redes sociais, em troca dos nossos dados? Acredito que não. Mas com certeza todos nós gostaríamos de sentir que temos controle sobre eles, que o Direito nos protege contra abusos, por mais que nós mesmos que tenhamos, de livre e espontânea vontade, fornecido nossa informação a um terceiro, seja do tipo cadastral, seja do que publicamos na web. Ganhará o mercado quem liderar a proteção da privacidade sustentável, com transparência. Qualquer outro formato, para um extremo do “libera geral” ou do extremo do “protege a pessoa dela mesma” está fadado ao fracasso. Até lá, por favor, vamos ler a regra do jogo que está no Termo de Uso dos serviços antes de dar OK.

DICAS PARA PROTEGER A PRIVACIDADE

- ✓ Leia os Termos e Políticas dos *sites* antes de se cadastrar.
- ✓ Veja se está claro para qual finalidade será usada sua informação e por quanto tempo.
- ✓ Se publicar informação mais pessoal nas redes sociais, faça-o de forma restrita, só para quem você autorizar poder ver e ter acesso.
- ✓ Evite publicar fotos (imagens) mais íntimas.
- ✓ Avalie sempre qual o preço que você está pagando por um serviço gratuito, seus dados têm valor.
- ✓ Quando cancelar um serviço, formalize por escrito (documento) que não quer mais que seus dados continuem a ser usados pela empresa.
- ✓ Faça uma lista de para quem você forneceu dados cadastrais.
- ✓ Oriente seus familiares para evitar publicar suas informações e fotos nas redes sociais sem sua autorização.
- ✓ Em caso de abuso, denuncie.

7.5. Identidade digital

A questão da prova de autoria desafia o Direito na era digital. Como saber quem está do outro lado da interface gráfica? A tecnologia tem nos ajudado a tentar determinar de forma mais inequívoca a identidade do indivíduo. No entanto, o ambiente de mobilidade da era Digital faz com que se enxergue apenas a biometria como forma de se ter uma autenticação mais válida. Mas como operacionalizar isso no acesso à Internet, ainda mais com o crescimento dos *hot spots* de *wi-fi* (*wireless*)? Como deve ser o modelo de identidade em um mundo plano, com fronteiras informacionais, em que não perguntar quem está passando pela porta virtual pode estimular a prática de ilícitos?

Esta discussão atinge desde a forma como o Brasil melhorou o padrão do documento de passaporte, o uso de coleta de digitais pela Polícia Federal, inclusive na imigração em diversos países, bem como a entrada em vigor do RIC — Registro Único de Identidade Civil, trazido pela Lei n. 12.058, anunciado pelo Governo Federal, para unificar os documentos de identidade. O documento seria similar a um cartão de crédito com *chip*, que reúne dados da cedu-

la de identidade atual, CPF e título de eleitor, podendo até ter informações de tipo sanguíneo e se a pessoa é doadora de órgãos. O mesmo será integrado ainda com sistema informatizado de identificação de impressões digitais, o AFIS. O RIC foi concebido com objetivo de integrar todos os bancos de dados de identificação do Brasil, inclusive podendo receber uma camada de biometria, além de um certificado digital.

Por causa da própria proibição constitucional do anonimato, tramita no Congresso o Projeto de Lei Federal do senador Gerson Camata (PMDB-ES) — PL 296/2008 (Senado) — PL 6.357/2009 (Câmara) — enviado para a Câmara dos Deputados em 5-11-2009, apensado ao PL n. 5.403/2001 — que busca implementar em todo país a exigência de identificação de usuário em cybercafé, *lanhouse* e assemelhados, prevendo ainda prazo de guarda de 3 anos destas informações (nome completo, documento de identidade, identificação do terminal utilizado, data e hora de início e término da utilização). O mesmo prevê multa de 10 mil a 100 mil reais dependendo da gravidade da conduta e reincidência, bem como cassação da licença de funcionamento do estabelecimento. O prazo para que as *lanhouses* e cybercafés se adaptem após a promulgação da lei é de 120 dias.

Definitivamente, um dos assuntos mais importantes a tratar no Direito é o tema da Identidade Digital obrigatória. Não adianta ter qualquer outra lei, se não pudermos gerar prova de autoria, seja para questões civis, criminais, trabalhistas, tributárias, entre outras. Isso deve ser consolidado, unificado, senão cada vez que para no Judiciário corre-se o risco de o juiz ter um entendimento distinto. Há juiz que entende que senha é suficiente para provar identidade, outros aplicam isso apenas quando há o certificado digital da ICP-Brasil, e há ainda os que dizem que só com assinatura do papel (como se isso trouxesse uma garantia maior, sendo que, na verdade, o papel é cópia quando a relação original foi manifestada no ambiente digital primeiramente).

Tabela com os Estados onde há lei para cybercafé e *lanhouse*:

UF	LEGISLAÇÃO	UF	LEGISLAÇÃO
ACRE	Não há	PARÁ	Não há
ALAGOAS	Lei n. 6.891/2007	PARAÍBA	Lei n. 8.134/2006
AMAPÁ	Lei n. 1.047/2006	PARANÁ	Não há
AMAZONAS	Leis ns. 3.173/2007 e 3.351/2008	PERNAMBUCO	Projeto de Lei n. 143/2007

BAHIA	Projeto de Lei n. 17.362/2007	PIAUÍ	Lei n. 5.747/2008
CEARÁ	Não há	RIO DE JANEIRO	Lei n. 5.132/2007
DISTRITO FEDERAL	Lei Distrital n. 3.437/2004	RIO GRANDE DO NORTE	Não há
ESPÍRITO SANTO	Lei n. 8.777/2007	RIO GRANDE DO SUL	Lei n. 2.698/2007
GOIÁS	Não há	RONDÔNIA	Não há
MARANHÃO	Não há	SANTA CATARINA	Não há
MATO GROSSO	Lei n. 8.502/2006	SÃO PAULO	Lei n. 12.228/2006
MATO GROSSO DO SUL	Lei n. 3.103/2005	SERGIPE	Não há
MINAS GERAIS	Projeto de Lei n. 1.720/2007	TOCANTINS	Não há

7.6. Direito comunitário e direito individual

A natureza da sociedade digital é comunitária. Saímos de uma sociedade agrícola-comunitária para uma sociedade industrial-individualista e entramos em uma sociedade digital-comunitária. Este processo vem sendo sentido desde o início do fenômeno da globalização, que começou há mais ou menos 500 anos, com a descoberta das Américas e o intenso comércio criado para fornecer produtos, bens e serviços à nova terra. A migração de pessoas, o avanço das comunicações e da tecnologia permitiram que o “Mundo Europa-Ásia” se transformasse em nossa atual Aldeia Global. A disputa pelos territórios geraram as guerras e criaram a geografia atual. Fenômeno semelhante está ocorrendo agora, só que no espaço virtual, no descobrimento e exploração da “Nova Terra Digital”.

Sendo assim, o Direito Digital é um direito comunitário por natureza. Entretanto, não estamos mais acostumados a viver em comunidade, no sentido da preocupação e grau de dependência do indivíduo com relação ao grupo, que faz com que o interesse particular seja preterido em prol do interesse coletivo.

O homem mais primitivo, que vivia em uma sociedade de base agrícola, tinha muito mais consciência coletiva e espírito comunitário do que nós temos atualmente, até por uma questão de necessidade de sobrevivência, onde o grupo determinava e garantia a segurança de cada um de seus indivíduos.

Apesar deste desafio do mundo moderno, o conceito de comunidade em termos de aplicabilidade jurídica continua muito presente na Comunidade Europeia. Grande parte das inovações jurídicas em termos de Direito Digital tem referência em modelos adotados na Europa. Isso se deve ao fato de que a consciência de comunidade é fator determinante para se poder ter boas leis em Direito Digital, em que a convergência de várias culturas e sua interpretação precede a norma. Os valores a serem protegidos são determinados dentro de um espaço social maior que os limites do território do Estado, o que exige uma flexibilidade da norma e uma dinâmica de equilíbrio com métodos de solução por autorregulamentação que são essenciais para o Direito Digital. Por isso estão tão avançados, em termos de Internet como um todo, com Diplomas Normativos Supranacionais e Diretrizes Gerais¹⁹ que permitem legislar sem prejudicar a evolução da própria rede, dos negócios, do mercado e da sociedade.

Sendo assim, o avanço tecnológico vivenciado pela humanidade no último século permitiu a construção da atual Sociedade Digital, baseada na eletrônica e nos ativos intangíveis, dependente dos insumos de energia, telecomunicações e tecnologia. Mas será que teríamos chegado até aqui sem um papel forte do Estado na vida das pessoas? Desde uma tribo indígena até as próprias redes sociais, os valores são codificados em regras coletivas impostas a cada participante daquela determinada comunidade. O Direito, em linhas gerais, prioriza a vontade coletiva sobre a vontade particular, em especial no que tange a segurança social. A liberdade de expressão e a livre-iniciativa são princípios fundamentais, mas podem ser preteridos em favor de um bem maior, dentro do desafio de criar sustentabilidade e governança pública em um cenário cada vez mais competitivo e de recursos ambientais escassos. Sendo assim, será que vamos evoluir para um mundo com mais controles ou com mais liberdades?

No Brasil, o cidadão não tem o direito de tirar a própria vida, pois é um direito *erga omnes* (acima da vontade do homem). Há um paradoxo natural entre o livre arbítrio e a proteção do Estado. As próximas gerações terão que fazer a difícil escolha entre ter mais privacidade ou mais segurança coletiva.

19. Citamos como exemplos a Diretriz 2.000/31 da Comunidade Europeia que dispõe sobre comércio eletrônico (Directive 2.000/31/EC on electronic commerce adopted in 8 June 2000), o Relatório da Comunidade Europeia sobre comércio eletrônico de 28 de fevereiro de 2000 e o Relatório do Comitê da EU sobre Crimes na Internet (European Committee on Crime Problems), de 2 de outubro de 2000.

A Sociedade Digital é uma aldeia global conectada. O indivíduo de hoje por certo tem mais voz e opinião do que uma pessoa de 2 mil anos atrás. Vivenciamos um momento de maior transparência e de mais informação, em que o acesso democrático ao conhecimento²⁰ proporcionado pela Internet permite que façamos melhores escolhas.

No entanto, estamos em um planeta de recursos escassos, onde há necessidade de não apenas decidir sobre o momento presente, dentro de uma ótica individual, mas também, por uma questão de sobrevivência, desde sempre, planejar o futuro, investir em questões que possam garantir melhores condições de existência humana na Terra, de convivência social, tais como segurança, saúde, habitação, alimentação, trabalho e educação. Nesse sentido, podemos dizer que a realização individual depende diretamente das escolhas coletivas: o que é feito visando o todo permite que uma pessoa possa ter mais chances de garantir sua própria felicidade.

A necessidade de um Estado que possa proteger o indivíduo e permitir seu crescimento e desenvolvimento pessoal é antiga. De certo modo, a noção de Estado nasceu dentro do próprio conceito de família, quando ainda éramos nômades, muito antes da própria Revolução Agrícola. A escolha de um líder e a obediência a ele ocorre inclusive com os outros animais, que criam modelos sociais para enfrentar a lei da selva, que é a lei do mais forte. Por isso, a Humanidade optou há muito tempo por construir um Estado de Direito²¹, substituindo o Estado de Natureza, sustentado em regras de conduta.

Apesar da aparência de modelo ideal, o Estado pode se tornar ilegítimo, quando não representa mais a vontade da maioria de um povo, quando o poder que deveria proteger passa a ser utilizado para oprimir. O Estado Opressor já

20. "O conhecimento tornou-se, hoje mais do que no passado, um dos principais fatores de superação de desigualdades, de agregação de valor, criação de emprego qualificado e de propagação do bem-estar. A nova situação tem reflexos no sistema econômico e político. A soberania e a autonomia dos países passam mundialmente por uma nova leitura, e sua manutenção — que é essencial — depende nitidamente do conhecimento, da educação e do desenvolvimento científico e tecnológico." TAKAHASHI, Tadao (org.). *Sociedade da informação no Brasil*: livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: <<http://www.mct.gov.br/index.php/content/view/18878.html>>. Acesso em: 30-5-2012 às 11h20.

21. "Estado é uma ordenação que tem por fim específico e essencial à regulamentação global das relações sociais entre os membros de uma dada população sobre um dado território, na qual a palavra ordenação expressa a ideia de poder soberano institucionalizado. O Estado, como se nota, constitui-se de quatro elementos essenciais: um poder soberano de um povo situado num território com certas finalidades. (...) Uma coletividade territorial, pois, só adquire a qualificação de Estado, quando conquista sua capacidade de autodeterminação, com a independência em relação a outros Estados." SILVA, José Afonso da. *Curso de direito constitucional positivo*. 10. ed. rev. São Paulo: Malheiros, 1994, p. 100.

se apresentou diversas vezes na história, mais recentemente nas Ditaduras que ainda persistem em países da América Latina, China, Oriente Médio, África.

O Estado é apenas um meio, um mecanismo para criação e distribuição de riqueza, não pode e não deve nunca ser um fim em si mesmo. Quando isso ocorre, há uma ruptura. Por certo é mais fácil dominar quando há menos informação. Por isso, há uma tendência de cada vez mais ser questionado o papel do Estado. Principalmente com o crescimento do terceiro setor e da mobilização social, potencializada pelo poder da internet, da manifestação e do protesto público digital.

Na busca de um equilíbrio que evitasse que a distorção do modelo pudesse criar um Estado tirano e arbitrário, muitos países implementaram o princípio tripartite de poderes: Executivo, Legislativo e Judiciário²², cuja independência e autonomia são condições *sine qua non* para garantir a própria liberdade. Nesse sentido a própria imprensa se tornou essencial para coibir abusos de autoridades.

Por outro lado, diversos estudos mostram que o excesso da liberdade também gera consequências danosas ao indivíduo, segundo Eduardo Benzatti “pela psicologia, quando há escolhas demais, as pessoas ficam infelizes. Em que medida liberdade em excesso não faz com que o indivíduo perca o chão”²³.

Quais são as principais questões que demandam grande reflexão para evolução do formato atual da relação indivíduo-Estado, até então mais protectionista e paternalista, para outro que seja de maior liberdade individual?

A primeira questão envolve educação. Há necessidade de que uma pessoa tenha uma formação básica, rica em valores éticos, para que possa ter maior discernimento na tomada de decisões. Ou seja, o direito de escolha depende diretamente da capacidade de se desenvolver visão crítica, análise, diagnóstico, estudo de cenários, gestão de risco, opinião. Deixar alguém decidir, sozinho, com informações erradas ou incompletas, e tendo ainda dificuldade de raciocinar em cima de fatores complexos e ecléticos, em um cenário de mudanças constantes, é extremamente prejudicial.

22. “O Estado, como estrutura social, carece de vontade real e própria. (...) Os órgãos do Estado são supremos (constitucionais) ou dependentes (administrativos). Aqueles são os a quem incumbe o exercício do poder político, cujo conjunto se denomina governo ou órgãos governamentais. Outros estão em plano hierárquico inferior, cujo conjunto forma a Administração Pública, considerados de natureza administrativa. (...) Vale dizer que o poder político, uno, indivisível, indelegável, se desdobra e se compõe de várias funções, fato que permite falar em distinção das funções, que fundamentalmente são três: a legislativa, a executiva e a jurisdicional.” SILVA, José Afonso da. Curso..., cit., p. 109.

23. Eduardo Benzatti. *A educação e os educadores do futuro*. Disponível em: <http://www.dominiopublico.gov.br/pesquisa/DetalheobraForm.do?select_action=&co_obra=105128>.

Nesse sentido, o direito ao voto é o exercício máximo da liberdade e deveria ser levado muito mais a sério. Até porque, depois, em um Estado Democrático, o sufrágio é a forma de representação popular que vai determinar a condução de um povo, seja pelas leis, seja pelo governo.

Logo, sem uma boa educação, não somos capazes de fazer boas escolhas e o voto se transforma em uma ferramenta de manobra e manipulação. E este é o primeiro grande problema na relação Estado-cidadão, especialmente no Brasil.

Em seguida, considerando que há necessidade de estabelecer regras de convivência social, há temas que precisam ser profundamente estudados, são eles:

- ✓ Privacidade do Indivíduo x Segurança Pública Coletiva
- ✓ Liberdade de Expressão x Responsabilidade
- ✓ Identidade Obrigatória x Anonimato
- ✓ Proteção de Dados x Acesso a Informação
- ✓ Crimes Digitais (novos tipos penais)

Estes são os grandes temas do Direito Digital, ou seja, do Direito aplicado a um modelo socioeconômico-político-jurídico de Sociedade que se manifesta de forma não presencial, por meio de testemunhas-máquinas, provas eletrônicas, e na qual o modelo de riqueza é a informação, sem fronteiras físicas ou temporais, em tempo real.

No tocante à privacidade, como veremos em capítulo próprio, a seguir, a Constituição Federal de 1988, em seu art. 5º, X, garantiu a proteção do indivíduo, em especial de sua vida privada, honra, imagem e reputação. Interessante que, em uma primeira análise, já se verifica o desafio desta garantia quando confrontada com o direito a liberdade de expressão. Mas isso ficou resolvido na mesma norma, em seu art. 5º, IV, que determina a livre manifestação de pensamento, mas proíbe o anonimato, assumindo a presunção de que todos podem falar o que pensam, porém respondendo pelo que dizem.

Portanto, em apenas dois artigos da Lei Magna de nosso ordenamento jurídico, há uma tentativa de se harmonizar a vontade do indivíduo (privacidade, liberdade, anonimato) com a necessidade de proteção dos demais, do coletivo (segurança, responsabilidade, identidade obrigatória).

Com a aprovação no Brasil da Lei de Acesso a Informação, ou LAI, Lei n. 12.527/2011, o princípio que passa a vigorar no tocante aos dados que estão na Administração Pública e nas empresas de Economia Mista é o da publicidade e transparência (art. 3º, I), ou seja, toda informação nasce pública e só terá seu acesso protegido se estiver enquadrada nas hipóteses legais que justifiquem essa medida de segurança (previstos nos arts. 23 e 24 do mesmo diploma legal).

Isso demonstra a cobrança do próprio povo brasileiro para que o Poder Público cumpra com o dever de assegurar a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação. Apenas excepcionalmente as informações serão protegidas, em princípio, só nos casos em que estiverem arroladas como sigilosas, se representarem um risco à segurança ou à soberania nacional, ou se já estiverem protegidas por outra lei, como ocorre com o segredo de justiça e com o segredo industrial, este último previsto na Lei n. 9.279/96.

Do outro lado, tem crescido a discussão de projetos de lei de proteção de dados sensíveis, de forma a complementar o próprio Código de Defesa do Consumidor, no que diz respeito ao uso dos dados dos indivíduos, seja por empresas privadas ou públicas. A tabela abaixo demonstra o crescimento de importância desta temática na América Latina:

PROTEÇÃO DE DADOS PESSOAIS — LATAM					
PAÍS	STATUS LEI OU PL	PAÍS	STATUS LEI OU PL	PAÍS	STATUS LEI OU PL
Argentina	Sim. 25.326 — 2000.	El Salvador	Nem em discussão.	Panamá	Nem em discussão.
Barbados	Lei de Prot. de Dados — 2005.	Guiana Francesa	Sim. A que vigora na França. Lei de Processamento de Dados desde 1978.	Paraguai	1.682-2001.
Belize	Nem em discussão.	Guatemala	Em discussão, n. 4090-2009.	Peru	Em discussão, n. 4079-2009
Brasil	Em discussão, mas não como projeto de lei.	Guiana	Nem em discussão.	Suriname	Nem em discussão.
Chile	19.628 — 1999.	Honduras	Nem em discussão.	Trinidad e Tobago	Em discussão desde 2011 Jan.
Colômbia	Projeto de lei do Senado n. 184 — 2000.	Jamaica	Nem em discussão.	Uruguai	Lei n. 18.331 — 2008.
Costa Rica	Lei n. 8.968 — 2011.	México	Sim. Desde 2010.	Venezuela	Nem em discussão.
República Dominicana	Nem em discussão.	Nicarágua	Em discussão, n. 5378-2008.		

Esses dados poderiam parecer até contraditórios, considerando a LAI, recentemente aprovada, mas não são. Pois, por um lado, há a transparência da informação nos Órgãos Públicos, e, por outro, a necessidade de proteger o cidadão de abusos no uso de seus dados. Isso porque há hoje uma grande

oferta de serviços gratuitos, mas que na verdade são pagos com informações que depois são utilizadas muitas vezes para propósitos que o usuário nem imagina.

Como viabilizar o direito ao protesto pacífico na Internet e ao mesmo tempo garantir a segurança dos internautas, coibindo ações que tiram do ar websites de serviços de utilidade pública prejudicando milhares de pessoas? Como exposto, há um limite bem sutil entre liberdade e abuso, e isso só consegue ficar mais bem definido com investimento em educação, que foi o primeiro ponto que apontamos como essencial para garantir a própria liberdade.

Pegando este gancho, entramos na discussão da necessidade de novas leis que tipifiquem os crimes digitais, que, em muitos casos, são apenas um novo *modus operandi* de um crime antigo, já previsto no Código Penal, mas, em algumas situações, trazem uma nova conduta, não tratada ainda como ilícita pelo Ordenamento Jurídico. Por exemplo, o crime de se criar um vírus ou o de disseminar um arquivo malicioso, ou mesmo o de invadir uma rede ou um computador, ou mesmo o celular de uma pessoa para obter dados.

Desde 1999 o Brasil discutia o Projeto de Lei de Crimes Eletrônicos²⁴, e nem os ataques das quadrilhas fizeram o projeto andar, como fez o efeito “Carolina Dickmann”, em que o vazamento de fotos íntimas de uma celebridade trouxeram à tona novamente a importância de se aprovar uma lei como esta. Isso porque a liberdade de um vai até onde não fira o direito de outro. Mas é bem difícil legislar sobre a matéria, pois é necessário conhecimento técnico. Além disso, o computador não consegue, como testemunha que é, diferenciar uma conduta dolosa (com intenção) de uma culposa (sem intenção), o que faz com que haja possibilidade de criminalizar condutas que em tese seriam de inocente (ex: mandar um vírus de computador para outra pessoa sem querer).

Precisamos aprender a usar a tecnologia de forma ética, segura e legal. A liberdade não pode se tornar uma bandeira para proteção de criminosos. O anonimato, por si só, estimula prática de ilícitos. Há necessidade de que o Estado tenha uma atuação social forte, mas que garanta a livre-iniciativa com o mínimo de intervenção possível.

Concluindo, independentemente do modelo que se adote no futuro para melhor regular a relação entre o Estado e o indivíduo, sabemos que a perda da crença na própria Justiça pode criar uma próxima geração, herdeira da geração Y, que faz justiça com o próprio *mouse*. E aí, teremos voltado para o Estado de

24. Ver Lei n. 12.734 (Lei Azeredo) e Lei n. 12.737 (Lei Carolina Dieckman), aprovadas em 30-11-2012.

Natureza, e isso será um grande retrocesso. A informação tem que construir e não banalizar, deve estimular a evolução da humanidade cada vez mais solidária e comprometida. O excesso do individualismo nos torna mais animais. Como dizia Thomas Hobbes, “o homem é o lobo do homem”. Daí a importância do estudo do Direito Digital para melhor interpretar a realidade em que vivemos.

7.7. Conciliação e enfrentamento

A solução amigável dos conflitos não é uma questão de alternativa jurídica no mundo digital; é uma das únicas vias sustentáveis dentro da dinâmica imposta pela velocidade de mudanças tecnológicas. A partir desse raciocínio, consideramos que a solução mais célere e eficiente para resolver questões de Direito Digital é a aplicação da mediação e arbitragem²⁵. Para as questões em que não se puder aplicar a arbitragem, como as questões penais, encontramos guarida em um modelo misto que possa incluir uma jurisdição virtual, como a que já vem sendo aplicada por vários países.

O Direito Digital atua em ambiente global, num regime de alianças e parcerias, com uma estrutura de mercado de “coopetição”, ou seja, competição mais cooperação. Portanto, a rivalidade que atinge as partes em lide deve ser sempre evitada, uma vez que a sociedade digital tem relações de dependência e efeitos em cascata muito maiores, pois estamos todos conectados. O preço a ser pago pelo desgaste de uma ação judicial é muito alto, devido ao custo do tempo, da mudança e da competitividade. A arbitragem possibilita que as partes cheguem a um acordo, visto que uma disputa jurídica significa perda para ambas. É um processo rápido, sigiloso e com a participação de mediadores e árbitros que entendem do assunto em discussão.

A Lei de Arbitragem — Lei n. 9.307/96 — permite que sejam incluídas cláusulas arbitrais em contratos²⁶. Esse procedimento deveria ser adotado em todos os contratos virtuais, seja de *e-commerce*, leilão, serviços ou informações.

25. A arbitragem no Brasil é atualmente regulamentada pela Lei n. 9.307, de 23 de setembro de 1996, que traz benéficas alterações ao instituto, anteriormente regulado pelo antigo Código Civil (Lei n. 3.071/16) e pelo Código de Processo Civil, arts. 1.072 ao 1.102 (revogados). Com a nova lei, já não há diferenciação entre arbitragem nacional ou internacional, pois se submetem às mesmas regras. O novo Código Civil trata da matéria em três artigos, 850 a 852, e não difere substancialmente do que dizia o Código anterior, porém foi feliz o atual legislador, que, ao revisar o projeto, teve o cuidado de incluir no art. 853 dispositivo que prevê lei especial para a matéria. Portanto, o novo Código Civil não revogou a Lei n. 9.307, de 1996.

26. Lei n. 9.307, de 1996, art. 4º, § 1º: “A cláusula compromissória deve ser estipulada por escrito, podendo estar inserta no próprio contrato ou em documento apartado que a ele se refira”.

Assim, ocorrendo um problema, as partes estariam aptas a eleger um árbitro para decidir a questão. As Câmaras de Comércio já contam com um rol de árbitros, assim como as associações de empresas de tecnologia e a própria Anatel. Portanto, é uma solução já usada e que poderia tornar-se regra. Como todo tipo de solução, tem aspectos positivos e negativos. No entanto, os aspectos negativos são muito menores que o prejuízo do tempo que causa a ida aos Tribunais e a burocracia judiciária²⁷.

7.8. Autorregulamentação

O Direito Digital tem como princípio normativo a Autorregulamentação, ou seja, o deslocamento do eixo legislativo para os participantes e interessados diretos na proteção de determinado direito e na solução de determinada controvérsia. Sendo assim, o Direito Digital possibilita uma via paralela que não a via legislativa para criar regras de conduta para a sociedade digital ditadas e determinadas pela própria sociedade.

A autorregulamentação parte do pressuposto de que ninguém melhor que o próprio interessado para saber quais são as lacunas que o Direito deve proteger, quais são as situações práticas do dia a dia que estão sem proteção jurídica e que caminhos de solução viável podem ser tomados. Um bom exemplo de autorregulamentação são os provedores de serviço de acesso à Internet, que têm contribuído e criado normas-padrão²⁸ a serem seguidas não apenas em nível local mas, principalmente, em nível global, no que tange às questões de privacidade e de crimes virtuais. A autorregulamentação já existe em nosso Direito há muito tempo. Uma série de categorias profissionais criam as suas próprias normas e diretrizes de trabalho, como a dos médicos, advogados e setores como o mercado publicitário e de Telecomunicações.

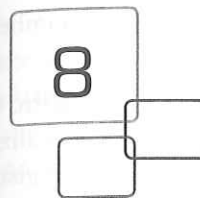
O princípio que norteia a autorregulamentação é o de legislar sem muita burocracia, observando a Constituição e as leis vigentes. Isso permite maior adequação do direito à realidade social, assim como maior dinâmica e flexibilidade para que ele possa perdurar no tempo e manter-se eficaz. Tal tendência

27. Além das vantagens enumeradas, o autor do projeto que redundou na Lei n. 9.307/96, o então Senador Marco Maciel, lembra-nos em seu texto *A arbitragem na solução de controvérsias* que o Juízo Arbitral é a solução mais justa e eficaz para dirimir conflitos entre empresas, firmas, fornecedores e consumidores de diversos países, em razão da sua capacidade de se amoldar aos diversos ordenamentos e sua validade não estar condicionada à territorialidade.

28. Lei de Introdução ao Código Civil, art. 9º, § 2º: “A obrigação resultante do contrato reputa-se constituída no lugar em que residir o proponente”.

de autorregulamentação por meio do exercício da liberdade responsável e das práticas de mercado sem intervenção estatal é uma das soluções que mais atendem à necessidade de que o Direito Digital deve não apenas conhecer o fenômeno social para aplicar uma norma, mas ter uma dinâmica e uma flexibilidade que a sustentem na velocidade das mudanças da sociedade digital que serão sempre sentidas, primeiramente pela própria sociedade.

Veremos, em vários capítulos do livro, a aplicação da autorregulamentação como solução de várias situações de conflito, da mesma forma que há minutas que trazem o princípio da autorregulamentação inserido, como é o caso das minutas no formato de *disclaimers*.



Novos Institutos Jurídicos de Direito Digital

8.1. Empresas virtuais e tendências da nova economia

Inicialmente, é importante ressaltar que Empresa Virtual não é o mesmo que extensão virtual de empresa real. Enquanto esta se refere a empresas que efetivamente existem no mundo real, física e juridicamente, aquela muitas vezes não conta sequer com uma sede física. Então, a primeira questão que se coloca quando falamos de empresas virtuais é definir sua existência jurídica¹.

Há empresas virtuais que têm por base um modelo de negócio adaptado do mundo real: a livraria virtual é um bom exemplo. No entanto, se essa livraria tem sua extensão no mundo real, ou seja, já é uma livraria consagrada, com marca conhecida e estabelecimentos comerciais físicos, ela é na verdade apenas extensão virtual de uma empresa real, ou seja, está mais para um PDV — ponto de venda — *online* que para um negócio de Internet. Por outro lado, no caso específico da Amazon, por exemplo, em que a livraria é um negócio virtual, em que não há lojas físicas, ou seja, ela não poderia existir sem a Internet, a relevância do formato jurídico é outra. No caso, devem ser observadas estratégias

1. Art. 45 do Código Civil: “Começa a existência legal das pessoas jurídicas de direito privado com a inscrição do ato constitutivo no respectivo registro, precedida, quando necessário, de autorização ou aprovação do Poder Executivo, averbando-se no registro todas as alterações por que passar o ato constitutivo”.

jurídicas específicas, não apenas para atender a suas necessidades, mas também para proteger os consumidores.

Frise-se, por oportuno, que muitos *websites* nem sequer têm Cadastro de Contribuinte ou qualquer registro em Cartório², o que dificulta a sua localização física quando há problemas com consumidores. Essa ausência de registro pode inviabilizar uma série de realizações comerciais, principalmente com fornecedores, investidores e financiadores. Há empresas virtuais que não conseguem assinar um contrato de locação de imóvel nem conseguem um seguro-fiança, pelo simples fato de não serem consideradas empresas tradicionais. Essas implicações nos levam a verdadeiras distorções e até a discriminação diante desse novo tipo de entidade jurídica.

Outro caso que merece destaque é o de empresas reais cujo modelo de negócio surgiu com o advento das novas tecnologias, especialmente da Internet, como é o caso dos provedores de acesso e dos provedores de serviços. A modalidade de Portais de Internet e de *Sites* de Busca também tem suas particularidades, uma vez que nenhum deles presta serviços que se enquadrem nas modalidades de objeto social e razão social conhecidas. Ou seja, tiveram de ser inventadas, concebidas pelo Direito Digital para atender a novas necessidades da sociedade.

É importante observar que o principal problema enfrentado é quanto ao correto enquadramento dessas empresas para fins de recolhimento de tributos, já que há distinções no caso de empresas de serviços, empresas comerciais ou empresas de tecnologia. Para fins tributários é essencial a determinação do tipo de empresa da melhor forma possível.

Independentemente do formato que a empresa digital venha a assumir, se o de empresa virtual ou de extensão virtual de empresa real, há problemas e desafios que se aplicam a qualquer empresa que se aventure no mundo virtual, seja na Internet, seja na convergência de novas mídias, como telefone e TV Interativa. O principal desafio é ter infraestrutura e logística preparadas para atender um cliente a qualquer tempo, em qualquer lugar, de qualquer cultura, dentro de qualquer legislação. Isso exige uma estratégia jurídico-comercial que ou atenda a toda a complexidade de se estar com a porta aberta para o mundo vinte e quatro horas por dia, ou delimite claramente as extensões de sua atuação e de sua responsabilidade jurídica.

Convém ressaltar ser grande falácia assumir que todas as empresas que quiserem ser modernas devem ter uma existência virtual. Em alguns casos, a virtualidade, ou seja, a presença na Internet, é absolutamente desnecessária, se não inadequada e até comprometidora: por exemplo, se uma empresa trabalha vendendo artigos com sucesso para determinada vizinhança, dentro de uma estrutura pequena, abrir uma extensão virtual não significa aumentar sua clientela. No caso, os velhos panfletos distribuídos pela vizinhança têm muito mais valor, pois atingem diretamente os clientes que interessam. Colocar essa empresa na rede significaria atingir usuários do mundo todo a qualquer hora e, para isso, é preciso estar preparado para atendê-los, o que exige grande investimento, que não necessariamente será pago pela empresa dentro de um modelo de rentabilidade e lucro. Ou seja, a virtualidade pode até comprometer o modelo de negócios e levar a empresa à falência, o que realmente chegou a acontecer com muitas empresas de Internet que não souberam administrar o custo-benefício de ter presença virtual-global e foram levadas à bancarrota com a queda do "Boom" das empresas de *Web*.

Um dos principais pontos de preocupação para essas empresas, que dependem diretamente de uma cadeia de fornecedores, notadamente as empresas de *e-commerce*, é a questão do controle de estoque. Isso porque, além do fato de ter que ter a capacidade de atender aos pedidos, há distinções jurídicas quanto ao seu formato e responsabilidades específicas, no caso de elas optarem por trabalhar com estoque próprio ou de terceiros. Dependendo da estratégia tomada, caberá a responsabilidade direta, única e exclusiva, da empresa em garantir a existência de determinado produto a seus consumidores³. Por isso, de modo a diminuir os riscos de ações jurídicas movidas por consumidores, uma das principais medidas preventivas é manter os usuários-clientes sempre informados sobre a disponibilidade do produto e sobre o tempo necessário para a entrega, e sobre quem é o responsável pelo estoque, por seu gerenciamento e pela entrega da mercadoria. Assim, estando ciente o consumidor é mais fácil diminuir o grau de insatisfação, um dos motivos que mais levam a ações judiciais em matéria de Direito do Consumidor.

Outro desdobramento que merece destaque em termos de logística é a questão da estrutura para atender um consumidor a qualquer momento, em qualquer lugar. Grandes *sites* devem trabalhar com *call-center*, com atendimento a clientes vinte e quatro horas, e manter visível na tela um telefone para

2. O Registro Público de Empresas Mercantis e Atividades Afins é regulado pela Lei n. 8.934, de 18 de novembro de 1994, que, por sua vez, é regulamentada pelo Decreto n. 1.800, de 30 de janeiro de 1996.

3. Depreende-se tal princípio dos arts. 30 e seguintes da Lei n. 8.078, de 1990 — Código de Defesa do Consumidor.

contato em caso de problemas com seus produtos ou com seu atendimento. O fato é que, no mundo real, o atendimento vinte e quatro horas é um diferencial, como no caso das lojas de conveniência, que por isso podem até cobrar mais caro pelos produtos vendidos; no mundo virtual, é uma exigência. Essas empresas têm a responsabilidade jurídica e o compromisso comercial de estarem preparadas para dar conta das demandas de usuários de diferentes culturas. Se isso não for possível, uma solução recomendável é deixar bem claro e com destaque no *website* os limites geográficos de seu atendimento. Novamente, a base de um negócio virtual bem-sucedido é a informação, quer seja sobre seus diferenciais de atendimento, quer seja sobre suas limitações comerciais e jurídicas.

Toda essa estrutura expõe outra falácia da rede: a de que montar um negócio virtual é bem mais barato que montar um negócio real. Em muitos casos, a logística virtual necessária é mais dispendiosa do que montar uma pequena loja. Por isso já dissemos que muitas empresas jovens da *web* foram pegadas de surpresa e fecharam por não estar bem assessoradas nesse sentido. No caso de empresas com existência real, o problema não é tão grande, pois normalmente elas já contam com sua rede de fornecedores e logística de atendimento e entrega montadas.

É claro que na categoria de empresas de serviços, que em geral não dependem tanto de fornecedores, a virtualidade pode realmente significar custos menores do que na modalidade de empresa real. A adequada colocação jurídica do contrato social e o adequado registro são dois fatores muito importantes para uma empresa virtual poder estar corretamente constituída. É importante destacar que várias delas, mesmo as que trabalharão exclusivamente com *e-commerce*, muitas vezes necessitam de excelente assessoria jurídica de negócios para atender à necessidade de criação de um novo conceito comercial, que possa enquadrar-se melhor em seu modelo de negócios, a criação de um novo formato jurídico e de cláusulas contratuais específicas que atendam às suas particularidades⁴. Por isso, a maioria dos casos em matéria societária e comercial em Direito Digital deve ser examinada individualmente, ou seja, a estratégia jurídica é determinada caso a caso, de acordo com as peculiaridades de cada negócio que se quer montar. A escolha errada da estratégia jurídica, como vimos, pode ser fatal.

4. Para exemplificar, valemo-nos da experiência societária do advogado Luiz Fernando Halembeck, que diz, no texto *Arranjos societários usuais em negócios de Internet*: “Em dez entre dez acordos societários em empresas de Internet os sócios acordam determinadas regras regulando a alienação de ações entre si ou a terceiros. As cláusulas mais frequentes envolvendo negócios de Internet são as cláusulas de direito de preferência, de aderir à venda de terceiros (*tag along*, *piggyback* ou *co-sale*) e de incluir na venda a terceiros as ações do outro sócio (*drag along*)”.

Uma consideração importante que devemos fazer quanto aos negócios virtuais é que empresas virtuais que não dão nota fiscal, principalmente no caso de prestação de serviços, como ensino a distância, em que a comprovação é dada via *e-mail*, contribuem para criar uma imagem de marginalidade da *Web*. Os negócios virtuais não devem ser tratados como se estivessemos em um mundo marginal, de camelôs virtuais. Esse tipo de atitude não traz benefícios para a expansão da rede como instrumento de negócios. A inadequada constituição jurídica, a falta de registros específicos, a volatilidade do negócio onde não há muita distinção entre uma empresa virtual e uma empresa fantasma geram insegurança que por sua vez faz com que o grande potencial comercial da rede não consiga ser totalmente explorado. A exigência de padrões comerciais deve ser cobrada, primeiro, pelas próprias empresas virtuais que estão regulares, pois são elas que acabam por sofrer com a falta de segurança e credibilidade gerada pela condição clandestina de muitos negócios virtuais.

Outra questão importante que merece nossa atenção é que toda essa volatilidade faz com que seja difícil até mesmo determinar a falência de algumas empresas virtuais. A maior parte do capital das empresas virtuais é capital humano, intelectual, então é muito difícil fazer uma liquidação ou uma execução judicial. A grande maioria, por não ter nem sede física, faz com que questões como de execução sejam muito difíceis. As empresas virtuais têm capacidade de assumir grandes responsabilidades, mas muitas não têm bens suficientes para garantir e honrar os compromissos, o que faz muitos donos de empresas virtuais terminarem por assumir a responsabilidade colocando em garantia seus próprios bens e não os da empresa.

Uma solução jurídica que enxergamos como viável seria a criação de cadastro virtual para consulta por todos aqueles que quisessem estabelecer um relacionamento comercial com a empresa virtual, como já acontece no mundo real. Nesse sentido, poderia também ser criado um processo de certificação por meio de uma associação que teria como escopo mostrar o grau de comprometimento da empresa virtual com questões de segurança, fornecimento de mercadorias, regularidade fiscal, entre outros. A principal consequência disso seria um aumento de credibilidade comercial e, portanto, de vendas, propiciado pela maior confiança que esses tipos de procedimentos permitem. Movimentos isolados não resolvem. Infelizmente, o mundo do comércio, seja ele real, seja virtual, é movido por condutas coletivas de mercado. Uma tendência é a da formação de associações comerciais virtuais, incluindo um *site* de serviços que possa informar suas atividades e os aprimoramentos que estão sendo buscados pelas empresas integrantes dessas associações virtuais de comércio.

Em termos conceituais, todo esse conjunto de atitudes para incentivar o aumento de credibilidade das relações virtuais pode ser chamado de *Disclosure*, que significa “Transparência”. Para citar uma referência desse padrão de conduta, tem-se o mercado de capitais norte-americano, que é o grande propulsor do desenvolvimento daquele país justamente por trabalhar este conceito: quanto mais informações tenho sobre determinada empresa, mais segurança tenho para investir em suas ações (isso vale até para investir, mesmo que a empresa esteja em baixa).

Um dos fatores mais prejudiciais para a credibilidade dos negócios virtuais é o excessivo grau de anonimato que a Internet propicia. Infelizmente, o mau uso do anonimato também por parte dos próprios empresários, para fins até mesmo de não pagamento de impostos, faz com que se forme uma espécie de “contracultura” comercial. Essa contracultura comercial, extremamente presente no Brasil, afasta investidores, consumidores e, principalmente, o *venture capital*, o capital de risco. O princípio do *venture capital* é não esperar resultados sempre, mas apostar em ideias — que são o princípio propulsor de uma economia sólida.

Nos Estados Unidos, o *venture capital* atua investindo em alunos das universidades — a semente, por exemplo, da Microsoft. Há grande interação entre iniciativa privada e mundo acadêmico. As incubadoras são formadas por empreendedores que querem executar suas ideias, muitas vezes dedicando anos de sua vida a elas.

É importante ressaltar que as incubadoras virtuais trouxeram para o Brasil novo formato de negócios. No entanto, em virtude de condutas inadequadas de alguns empresários imediatistas e da expectativa de lucro fácil associada à questão da “contracultura” comercial que já citamos, formou-se no Brasil uma espécie de “Incubadora às Avessas”, ou seja, de atravessadores de ideias, que não são empreendedores, mas comerciantes de ideias, que esperam receber dinheiro de investidores mas não têm nenhuma expectativa ou vontade de continuar no negócio a longo prazo. Por isso, neste caso, por prevenção, recomendamos aos investidores que em seus contratos de investimento coloquem como condição de realização do negócio a permanência e continuidade do criador dele até a sua consolidação ou por um prazo mínimo preestabelecido entre as partes. Esta é uma boa forma de farejar o quanto o autor daquela “ideia genial” quer empreender para levá-la adiante e o quanto ele quer passá-la para a frente. Juridicamente, o problema pode ser resolvido nos contratos entre a incubadora e o detentor do capital de risco, prevendo-se a recompra de parte dos títulos dentro de determinado prazo, quer seja pela empreendedora, quer seja pela própria incubadora. Tal tipo de contrato amarra o detentor da ideia para que ele se empenhe em que ela seja bem-sucedida no longo prazo.

O papel do Direito na sociedade é trazer soluções, por isso é um constante exercício de inteligência. Nem sempre leis trazem soluções, principalmente no âmbito digital, em que as características determinam que apresentem soluções específicas para cada caso concreto.

Devemos enxergar que o Direito Digital vem atender a uma nova sociedade, a Sociedade Digital. Que a mudança comportamental é plena, nos negócios, nas relações, nos Indivíduos. As mudanças não são peculiares apenas às empresas virtuais ou à Internet, mas sim a todo o ordenamento jurídico. Exemplo disso é a adoção cada vez mais frequente do “Regime de Coopetição” (cooperação mais competição). Esse novo regime de negócios reflete uma necessidade das empresas de cada vez mais buscar alternativas de sobrevivência em um mundo competitivo, globalizado e, principalmente, conectado. Empresas isoladas tendem a naufragar. Em termos de Direito Digital, isso significa que fica muito difícil distinguir parcerias estratégicas de operações de *trust* e monopolização de mercados. Até onde o formato de mercados B2B e metamercados verticais e horizontais atendem aos interesses dos consumidores também? São estas soluções ferramentas de sobrevivência inofensivas, ou comprometem os princípios econômicos que regem o capitalismo?

Agora façamos uma análise estrutural da Internet. Sua configuração física como uma rede com um emaranhado de conexões, a grande velocidade do tráfego de informações, as constantes mudanças que lhe são características, sua presença global fazem com que a competição desenfreada se torne verdadeira carnificina virtual, o que além de sair muito caro chega até mesmo, muitas vezes, a prejudicar não só as empresas como os consumidores. O fato de que o usuário da *web* tem de ser capaz de localizar o *site* da empresa entre tantas opções acaba provocando verdadeira disputa por visibilidade, uma Guerra de Comunicação. O volume absurdo de investimentos em publicidade gastos nessa batalha faz com que pouco sobre para investir em atendimento, melhoria de serviços, pesquisa, relacionamento. Nesse contexto, cooperar não significa deixar de disputar as fatias do mercado, mas sim não fazê-lo de forma predatória⁵. A postura predatória pode ser muito mais nociva no mundo virtual que no real.

5. Parafraseando ainda o já mencionado texto de Luiz Fernando Halembeck, podemos dizer que são comuns nas associações de Internet estipulações de exclusividade e não concorrência. As primeiras se aplicam aos sócios que administram o negócio e, dependendo do poder de barganha deste, podem estender-se ao acionista que fornece o capital.

Já as obrigações de não concorrência são admitidas no Brasil quando tiverem prazo e território definidos. Os prazos em geral são de dois a cinco anos após o desligamento do acionista da administração ou do capital da empresa.

É necessário frisar que, mesmo sendo uma rede com capacidade ilimitada, há certo limite no número de *players* que se estabelecerão com sucesso, como acontece em qualquer mercado. Quando há mais *players* do que o mercado pode absorver, podem ocorrer duas situações jurídicas distintas: falências generalizadas ou um grande número de fusões. Cada uma delas tem aspectos e particularidades jurídicas específicas, sobretudo no tocante às empresas que sejam puramente virtuais. O que se exige, como já vimos, são soluções medidas e estudadas caso a caso.

É importante ter claro que, como em qualquer mercado, a área virtual apresenta três estágios econômicos distintos: primeiro, a inovação, em que os pioneiros se estabelecem; depois, um inchaço, em que há uma multiplicidade de *players*. Finalmente, há a limpeza natural, em que só ficam os mais capacitados. Nada diferente de qualquer outro ciclo econômico do mundo capitalista. Por isso, ao contrário do que se pensa, a Internet não é um mercado do oportunismo, mas cumpre um ciclo comum no mundo capitalista. Estabelecida há muito pouco tempo, vive ainda uma etapa em que os três movimentos subsistem. Isto representa um emaranhado de problemáticas jurídicas para garantir direitos e obrigações dentro de um conjunto de participantes ainda não totalmente estabelecidos e definidos, que se relacionam e assumem compromissos e responsabilidades que nem sempre tem sustentação jurídica no tempo e no espaço.

A consequência disso é um processo doloroso, repleto de riscos, cuja tendência natural, porém, é encaminhar-se para um movimento de empreendedorismo, rejeitando o movimento puramente especulativo. Nesse caminho, as empresas jurídicas e estruturalmente bem resolvidas, dentro de padrões corretos que valem para o mundo real e o virtual, serão as que se consolidarão.

Isso se tem mostrado inclusive na mudança de método de avaliação dos negócios. Os ativos são cada vez mais intangíveis, como marca, *softwares*, bancos de dados, conteúdos, *know-how*. A expectativa de valor de uma empresa se dá por sua capacidade de aderência à realidade e, ao mesmo tempo, de inovação. É o que se verifica, por exemplo, na compra de diversos negócios da nova economia, como foi o caso de o Google adquirir o YouTube. O que se está comprando de fato? Um grande laboratório capaz de gerar informação preciosa, qualitativa, sobre o que os consumidores querem. Capaz ainda de gerar conteúdo, por parte dos próprios internautas. O que se busca ao comprar uma empresa de *software* que é detentora de determinados códigos-fonte, ou melhor, de determinados “gênios da tecnologia”? Para fins de análise jurídica, realizada muitas vezes em processos de *due diligence*, em que advogados das partes com-

pradoras e vendedoras avaliam o negócio, seus ativos e seus riscos para determinar as condições de compra e venda, ou de fusão e aquisição, estas questões são fundamentais. Por esse motivo, cada vez mais, investidores e empresas buscam a opinião de um advogado especialista em Direito Digital, capaz de analisar de modo profundo a realidade de um negócio da nova economia.

8.2. Provedores de acesso, de serviços e de conteúdos

O que é um Provedor de Acesso? Resumidamente, é uma empresa prestadora de serviços de conexão à Internet, agregando a ele outros serviços relacionados, tais como *e-mail*, *hosting* de páginas *web* ou *blogs*, entre outros, que detém ou utiliza determinada tecnologia, linhas de telefone e troncos de telecomunicação próprios ou de terceiros.

Mas o que torna os provedores tão importantes em termos jurídicos? É que os provedores de acesso não são apenas empresas prestadoras de serviço. São os grandes aglutinadores do mundo virtual, responsáveis pela abertura das portas de entrada dos usuários na rede (seja ela pública, como a Internet, ou privada, como as de acesso restrito). Isso significa que muitas das soluções jurídicas para a proteção de valores sociais e das relações interpessoais na rede têm seu início nos provedores e podem ser mais bem controladas por meio deles.

Inicialmente, vamos entender as características jurídicas da dupla atuação dos provedores de acesso. Há duas posições jurídicas bem determinadas. A primeira deve a sua atuação como Operadores de Telecomunicações responsáveis pela transmissão de mensagens e conteúdos por meio da rede. A segunda, de Editores responsáveis pela hospedagem, publicação e até produção de conteúdo na Internet. Cada uma dessas situações determina níveis de responsabilidade distintos⁶.

6. Enquanto o provedor atuar como mero conduto para o tráfego de informações, equipara-se às companhias telefônicas, não podendo ser responsabilizado por eventuais mensagens difamatórias transmitidas, já que não pode ser compelido a vistoriar o conteúdo de mensagens em cuja transmissão não tem participação nem possibilidade alguma de controle. No entanto, quando no caso concreto for possível detectar a presença de controle editorial, fica caracterizada a responsabilidade do provedor, à semelhança do que ocorre com o editor na mídia tradicional. Esta é a orientação dada pela Corte de Apelações do Estado de Nova York (*New York State Court of Appeals*) que se depreende de sua primeira manifestação sobre o assunto (em 2-12-1999).

As características dos serviços contratados dos provedores são custo, competência técnica, confiabilidade no plano de segurança, capacidade e quantidade de linhas disponíveis em relação ao número de usuários, o que significa que é uma modalidade de empresa relacionada com a área de telecomunicações⁷, mas com características próprias e peculiares ao veículo de comunicação Internet, que é não só meio, como mídia.

É importante ressaltar que a Internet, como qualquer rede, é acessada. Todo o conteúdo que está na Internet é acessado, ou seja, não existe uma materialização física dele para transportar seus direitos, como ocorre com livro, filme, CD ou DVD. Não existe o pedido de uma identificação (como a cédula de identidade) para que se entre em uma área pornográfica ou de acesso restrito a maiores de idade, como ocorre nas casas noturnas e discotecas. Mas existe a tecnologia. A Internet funciona como uma rede orgânica em que os responsáveis pelas portas de entrada e saída têm como autorizar o acesso, restringi-lo, identificar o usuário em seu banco de dados, entre outras informações⁸. Essa capacidade deve ser usada cautelosamente, apenas para atender à exigência crescente de segurança da Internet, sem invadir a privacidade dos usuários.

Para o Direito Digital, a solução para questões de *e-commerce*, fraudes e pedofilia está na orientação para Autorregulamentação dos Provedores⁹, em

7. Quando consultado pela Procuradoria-Geral da Fazenda Nacional (Parecer PGFN/CAT/N. 1.093/97), questionando se a Internet é ou não serviço de comunicação, o Sr. Ministro de Estado das Comunicações subscreeve o Aviso 173/MC informando: “com relação ao assunto, informo a Vossa Excelência que a comunicação via INTERNET constitui serviço de valor adicionado, não sendo considerada serviço de telecomunicações (§ 1º do art. 61 da Lei n. 472, de 16 de julho de 1977)”. Também vale destacar que tal característica fez com que a Primeira Seção do Superior Tribunal de Justiça (STJ) decidisse que não incide Imposto sobre Circulação de Mercadorias e Serviços (ICMS) sobre os serviços prestados pelos provedores de acesso à Internet (EREsp 456.650). Ver a Súmula 334 do STJ, julgada em 13-12-2006 e publicada no DJ de 14-2-2007, p. 246, a qual versa em seu enunciado: “O ICMS não incide no serviço dos provedores de acesso à Internet”.

8. Nesse sentido, é interessante observar como os projetos de lei relacionados a tal fato (Projeto de Lei n. 3.016, de 2000, do Deputado Antonio Carlos Pannunzio; Projeto de Lei n. 3.891, de 2000, do Sr. Julio Semeghini; Projeto de Lei n. 4.972/2001, do Sr. José Carlos Coutinho; Projeto de Lei n. 7.461/2002, do Sr. Eni Voltolini; Projeto de Lei n. 1.256/2003, do Sr. Takayama; Projeto de Lei n. 480/2003, do Sr. Pompeo de Mattos; Projeto de Lei n. 880/2011, do Sr. Jonas Donizete) tentam regulamentar a captação e o arquivamento de informações sobre os usuários, realizados pelos provedores de acesso. Para que estas informações possam a qualquer momento ser solicitadas como meio de prova pela autoridade judicial. Destacamos que os projetos de lei aqui citados foram apensados a outros dois — PL n. 3.016/2000 em 25-6-2003, e PL n. 5.403/2001 (originariamente PLS n. 151/00) e este último está desde 10-3-2008 aguardando a criação de uma Comissão Especial.

9. Depois de muita discussão, de muitos avanços e retrocessos, o Conselho de Ministros da União Europeia (UE) aprovou a diretiva que obriga os provedores e as companhias opera-

âmbito internacional, por meio de um Código de Ética, Padrões e Procedimentos. Além disso, acreditamos que a regulamentação dos *Disclaimers* e sua adoção como formato-padrão de normatização digital pode ser um caminho viável para criação de Normas Digitais com controle e sanção imediatos permitidos pelo próprio *software* que identifica o “de acordo” do usuário e sua capacitação diante dos requisitos que tal norma determinar com base nos preceitos legais vigentes.

Em matéria de controle de conteúdo, seja qualitativo, seja quantitativo, enxergamos que uma solução adequada consiste em que, no momento da definição do contrato de hospedagem da página ou *website* com o provedor, seja definido quem é o responsável editorial pelo conteúdo a ser publicado pela pessoa física ou jurídica que está contratando os serviços de hospedagem para ter sua presença na Internet¹⁰. Isso não só limita a responsabilidade do Prove-

doras de redes de comunicação a reter os dados de tráfego de Internet e de chamadas telefônicas. A versão final da Diretiva sobre Retenção de Dados de Tráfego Telefônicos e de Comunicações Eletrônicas de 21 de fevereiro de 2006 foi aprovada por maioria, com o voto contrário dos ministros da Irlanda e da Eslováquia. O objetivo primordial da Diretiva, portanto, foi o de harmonizar essas legislações díspares. As diferenças de requisitos entre as leis nacionais, no que tange à retenção de dados, estavam impedindo o desenvolvimento do mercado das comunicações eletrônicas na Europa, tendo em vista que os provedores eram obrigados a lidar com diferentes exigências legais, no que diz respeito ao tipo de dados que deveriam ser arquivados e ao período de tempo do armazenamento deles. Uma diretiva anterior (5), do ano de 2002 — Diretiva 2002/58/EC (6) —, regulou especificamente a questão da privacidade no âmbito das comunicações eletrônicas. Uma versão do desenho final da nova Diretiva pode ser encontrada no site do “Registro Público dos Documentos do Conselho” da União Europeia, no seguinte endereço: <<http://jus2.uol.com.br/doutrina/texto.asp?id=8119>>.

10. Selecionamos, a título de exemplo, cláusulas de isenção de responsabilidade de um serviço de hospedagem de páginas, que ilustram perfeitamente a tendência da autorregulamentação e a questão da responsabilidade por conteúdos publicados *online*. O Termo de Serviço está disponível na íntegra no endereço <<http://www.hpg.ig.com.br>>:

“11. LIMITAÇÕES DE RESPONSABILIDADE E GARANTIA

11.1. O IG não será responsável perante terceiros pela utilização, tampouco pelo conteúdo dos *websites* criados por afiliados do Portal hpG. O hpG não é responsável por qualquer dano causado por perda de acesso, cancelamento, falta de armazenamento ou de cópia de segurança, ou modificações dos *websites* dos afiliados. Os afiliados são responsáveis pela manutenção, atualização e criação de cópias de segurança de seus *websites*.

11.2. O IG não será responsável e nem oferece qualquer garantia sobre a exatidão, veracidade, ou integridade das informações contidas nas páginas do Portal hpG inseridas por afiliados e não assume responsabilidade por (i) quaisquer erros ou omissões que resultem da utilização dessas informações; (ii) quaisquer falhas, atrasos ou interrupções no fornecimento de qualquer conteúdo incluídos na forma de ‘website’ no Portal hpG ou (iii) perdas ou danos da utilização do conteúdo ou dos serviços hpG proporcionados pelo IG.

(...)

12. INDENIZAÇÃO E LIMITAÇÃO DE RESPONSABILIDADE

dor como possibilita verdadeira limpeza no que é publicado irresponsavelmente na Internet. Não havendo um responsável, o conteúdo não vai ao ar. Esta seria uma forma de sanção dentro do princípio de Autorregulamentação.

Portanto, em termos de provedores de acesso, o mais importante é ter em mente que eles são uma nova modalidade de empresa dentro do segmento Telecomunicações com características mistas, já que também assumem responsabilidades editoriais, como veículo de informação e imprensa, e são o principal meio para criar soluções tecnójurídicas¹¹, que é quando a tecnologia se junta ao Direito para materializar um formato de instrução jurídica para o meio virtual.

Mas os negócios têm evoluído com a própria Internet, e novos modelos de provedores surgiram. Há hoje provedores de serviços apenas, que não fornecem nem acesso, nem tampouco conteúdo, como é o caso de um Google. E há provedores apenas de conteúdo, que também não fornecem acesso.

No entanto, os provedores de acesso continuam sendo as grandes portas de entrada no mundo virtual, e sua posição é privilegiada. Agora, com a mobilidade e com o advento da TV digital, já estão sendo criados provedores de mobilidade, bem como provedores de conteúdo para TV digital. A questão que se coloca é: quem vai ganhar esta briga?

8.3. Comércio eletrônico e e-Business

O comércio por via eletrônica já é muito antigo. Nesse sentido, é até pouco apropriado definir o comércio por operação via Internet como Comér-

12.1. O afiliado concorda em indenizar o IG contra toda e qualquer reclamação e despesas, incluindo honorários legais, resultantes da utilização indevida do serviço de criação e hospedagem hpG pelo afiliado, quando a referida indenização resultar de (i) a responsabilidade do afiliado por toda e qualquer obrigação resultante da violação ou infração de direitos de propriedade, autorais, marcas registradas, ou marcas de serviço e (ii) a responsabilidade do afiliado por toda e qualquer obrigação resultante de material difamatório ou ilegal contido no *website* do afiliado.

12.2. Ao utilizar o serviço hpG, você concorda em não responsabilizar o IG, suas afiliadas, administradores e funcionários por reclamações, queixas, direitos, obrigações, danos (efetivos, diretos ou indiretos), custos e despesas de qualquer tipo ou natureza, conhecidos ou desconhecidos, previsíveis ou imprevisíveis, divulgados ou não divulgados, que possa ter resultante, ou de qualquer forma, relacionado com essas reivindicações e/ou produtos e serviços hpG¹².

11. Solução tecnójurídica é aquela que traduz uma norma jurídica em linhas de programação e linguagem de computador, fazendo com que rotinas e *softwares* façam o papel de cumprir o que está legalmente determinado: ex.: pedir uma rotina de confirmação de dados para fazer um *download*.

cio Eletrônico, que é uma terminologia mais abrangente — inclui meios eletrônicos como um todo como fax, *machine-machine* etc. Mas, para fins didáticos, vamos utilizar o termo Comércio Eletrônico para definir as operações comerciais via Internet.

Para começar, muitas das questões atuais levantadas sobre operações de compra e venda na Internet e utilização de cartão de crédito são questões rotineiras que nos afligem quando usamos o cartão em lojas e restaurantes, quando fazemos compras por telefone ou catálogo. Tais questões, nada virtuais, ainda não têm solução e sua problemática, é claro, termina por estender-se às novas tecnologias e meios de comunicação, como a Internet.

As transações de comércio eletrônico não diferem das feitas por outros meios de comunicação remota como o telefone ou o fax. Mas, se para muitas pessoas ainda é difícil dar um número de cartão de crédito por telefone, quer seja para comprar algo pelos sistemas de telemarketing, quer seja pelo *marketing* direto de algumas empresas, imagine qual não é a dificuldade de fazer o mesmo por Internet — que, *grosso modo*, não passa de uma linha de telefone com interface gráfica. A incompreensão que ainda existe quanto ao meio é agravada pelo fato de ainda não ter sido estabelecido um padrão de conduta mais uniforme quanto à prova documental para as operações *online* em nível tão globalizado quanto é a Internet¹².

O Direito Digital busca resolver esta questão mediante a regulamentação dos documentos eletrônicos como instrumentos juridicamente aceitos para comprovar a veracidade das operações eletrônicas virtuais, procurando conseguir um alcance de vários ordenamentos, já que de nada adianta ter padrões distintos no Brasil, na Argentina, nos Estados Unidos, na Inglaterra, na Austrália — a operação pode ocorrer, até mesmo envolvendo todos ao mesmo tempo.

A sociedade digital já assumiu o comércio eletrônico como um novo formato de negócios. Já existem o *e-commerce*, o *m-commerce* e o *t-commerce*, dependendo se o veículo de transação eletrônica é um computador, um celular ou dispositivo de comunicação móvel, ou a televisão. A tendência é que esse formato se amplie cada vez mais, conforme a tecnologia se torne mais acessível, a rede mais estável e as normas-padrão mais aplicáveis.

12. A esse respeito, podemos citar a lei modelo da Uncitral — *United Nations Commission on International Trade Law* —, que serve de diretriz para todos os países a fim de que regulamentem o comércio eletrônico. A Uncitral determina que o uso de tecnologias de encriptação confere ao documento eletrônico o mesmo grau de segurança dos documentos escritos, fazendo jus então a igual tratamento no tocante ao valor probatório. Vários ordenamentos já adotaram o modelo da Uncitral, como o americano, o alemão, o francês, o argentino e o colombiano.

Uma das primeiras mudanças trazidas pelas práticas comerciais eletrônicas é a de conceito de produto. Este, em alguns casos, deixa de ter um aspecto físico, palpável, e passa a assumir a forma de serviço acessado, como já ocorre com livros (*e-book*) e música (mp3). Culturalmente, a insegurança do ambiente de rede é um dos maiores empecilhos para a expansão definitiva do *e-commerce*.

No âmbito do Direito Digital, os requisitos para garantir a segurança das relações comerciais realizadas eletronicamente são as informações, a transparência, o emprego padronizado da assinatura eletrônica de duas chaves assimétricas (com verificação simultânea do ID — Identidade Digital, ou seja, o cruzamento do código IP, *e-mail* e CPF do comprador para seu reconhecimento *online*) e o uso de seguros específicos para transações *online* com pagamento de prêmio — já que se paga seguro contra furto do cartão de crédito, seguro contra perda do celular, por que não pagar um seguro contra fraudes *online*?

Entendemos por informação e transparência a publicidade de dados específicos sobre a empresa que opera virtualmente, com informações sobre produtos e serviços, a lei e o ordenamento a que está submetida não apenas a empresa, mas o contrato de compra e venda eletrônico, se há cláusula de arbitragem ou se há a nomeação de um foro específico, se há seguro para operações *online*, qual o nível de atualização do *software* de segurança e as referências cadastrais e de mercado para consulta do consumidor, caso necessário.

O cumprimento da exigência de transparência de informação faz com que não se caia na modalidade de culpa *in omitterendo* do Direito Civil (CC, art. 186), que responsabiliza por danos causados devido à omissão de informações relevantes, estando este princípio também previsto pelo Código de Defesa do Consumidor¹³.

O dever de informação e de aconselhamento é, acima de tudo, um corolário da boa-fé que contribui para a defesa da empresa que tiver algum problema com seu consumidor. Como se vê, o bom funcionamento do comércio eletrônico pode ser solucionado pela aplicação da legislação vigente e de algu-

mas exigências de transparência e segurança que devem ser seguidas pelas empresas que operam nesse terreno.

As iniciativas de normatização do comércio eletrônico¹⁴ dispõem sobre uma série de quesitos para regular as transações na rede que já existem na legislação vigente, para as transações de mundo real. Esse tipo de situação vem demonstrar que ainda persiste um entendimento incorreto do que é o comércio eletrônico. Transações eletrônicas já existem há mais de vinte anos: envios de fax, transferências bancárias, compensação de cheques, cartões de crédito, cartões de débito, investimentos feitos por corretoras de valores, são todas transações eletrônicas. As operações citadas têm seu lado virtual e real: a parte virtual é a transação em si, ou seja, o deslocamento de dados por via eletrônica; a parte real são os participantes e os documentos impressos que comprovam sua realização.

O comércio eletrônico é apenas uma evolução da transação eletrônica. Permite que não apenas a transação seja virtual, mas também que seus partícipes e documentos comprobatórios permaneçam virtuais, que ambos se apresentem eletronicamente.

A questão nova se coloca, então, em termos de garantir a segurança dos participantes e a certificação de suas identificações, tópicos que abordamos nos capítulos anteriores. Todo o resto é uma questão de contratos entre as partes e de aplicação do Código de Defesa do Consumidor, quando se tratar de consumidor final. Uma legislação específica sobre o setor é desnecessária e não será capaz de acompanhar sua evolução tecnológica. Por isso, a nosso ver, normas-padrão que orientem no sentido da segurança da operação, como foi demonstrado, são o caminho jurídico mais adequado.

É importante compreender que o comércio eletrônico tem participantes virtuais, não limitados pela territorialidade e que fazem uma transação eletrônica entre si. Existe também uma documentação digital, que vale como manifestação de vontade — sejam contratos firmados virtualmente ou os próprios dados da operação armazenados nos computadores do remetente, do receptor e do interceptor, no caso dos Provedores.

13. A omissão de informações ao consumidor é coibida por diversos artigos do Código de Defesa do Consumidor (CDC), como, por exemplo, os arts. 18 e 20, que estabelecem como vícios do produto e do serviço, respectivamente, a disparidade destes com a mensagem publicitária; o art. 30 determina que as informações ou publicidade veiculadas pelo fornecedor vinculam este ao consumidor e integram o contrato que vier a ser celebrado; mas o dever de informar está plenamente descrito no art. 31 do CDC que diz: “Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores”.

14. Além do Anteprojeto de Lei da Ordem dos Advogados do Brasil, dispõem sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital o Projeto de Lei n. 672 de 1999 (arquivado), do Senador Lúcio Alcântara (apensado PL n. 4.906/2001), o Projeto de Lei n. 1.589 de 1999, do Deputado Luciano Pizzatto (apensado PL n. 1.483), e o Projeto de Lei do Senado n. 672, de 1999 (apensados PL n. 1.483/1999, PL n. 6.965/2002 e PL n. 7.093/2002).

Com o aumento do comércio eletrônico e o aumento do acesso à Internet, outra modalidade começou a ganhar força: as compras coletivas nada mais são que um *site* que concentra ofertas diárias (por exemplo, um jantar em um restaurante cinco estrelas) com desconto bastante atrativo para conquistar clientes. As ofertas geralmente precisam de um número determinado de vendas para ser validadas. O baixo custo devido aos descontos conquistou logo diversos usuários da *web*. Todavia, é necessário que o consumidor esteja atento às condições de compra e uso das compras que fizer, por exemplo, verificar se o restaurante ou o estabelecimento comercial possui capacidade suficiente para atender diversos clientes, devendo o *site* de compras coletivas, por sua vez, ressarcir o usuário caso a oferta não seja alcançada. O ideal é que o consumidor guarde todos os documentos comprobatórios da sua compra para evitar quaisquer problemas futuros.

A moda das compras coletivas surgiu no Brasil em 2009, mas foi só em 2012 que estes *sites* de comércio eletrônico ganharam popularidade. Isso porque nós, brasileiros, adoramos receber grandes ofertas, mas até que ponto podemos confiar nesses *sites*? Da mesma forma que realizamos compras em *sites* ou até mesmo em lojas físicas, é necessário estar atento na hora de realizar a compra.

A mecânica é bem simples: a oferta do produto ou serviço é lançada no *site* e, quando atingir um número mínimo de consumidores, começa a valer. Essas ofertas mudam diariamente, de acordo com a localização do consumidor, buscando fidelizar clientes.

O consumidor tem que estar atento, pois, no momento em que se adquire o cupom, é firmado um contrato entre as partes. E, em Direito, o princípio de que os contratos devem ser cumpridos também prevalece entre *sites* e consumidores. O serviço que foi ofertado deve ser bem atendido, assim como na aquisição de produtos.

Já as empresas também têm que estar preparadas nos casos em que houver reclamações dos consumidores, e estas tendem a crescer ainda mais em tempos de redes sociais e mobilidade. As reclamações surgem a partir de *e-mails* para o próprio *site* de compras coletivas, podendo-se usar até os *sites* de reclamação e dos órgãos de proteção ao consumidor e redes sociais. Por isso é importante investir também em atendimento ao consumidor. Há jurisprudências e um projeto de lei¹⁵ que prevê a regulamentação das compras

coletivas, mas não deve prosperar, pois tal norma é bastante restritiva, sendo que esse setor é bastante dinâmico, e limitaria também a inovação das próximas gerações deste negócio.

Devemos frisar que, em último caso, é a atitude dos consumidores que determina a conduta das empresas, quer no mundo real, quer no virtual. Por isso é preciso que fique claro para os consumidores que seus direitos, numa transação de comércio eletrônico, são os mesmos que no mundo real¹⁶. Assim também é para os deveres das empresas: ela tem de informar em que território se localiza e como resolverá eventuais problemas com seus produtos nos territórios para os quais vende¹⁷. O ideal é que todo *site* tenha claramente informado um telefone de contato, quem são os seus representantes em outros territó-

“Consumidor. Responsabilidade civil objetiva. *Site* de compra coletiva. Oferta de aparelho celular vinculado a plano de utilização da linha telefônica. Aquisição de cupom sem a respectiva entrega do produto. Falha na prestação do serviço. Dano moral configurado. Precedentes deste TJERJ. Responsabilidade solidária dos integrantes da cadeia de consumo. Verba reparatória fixada em conformidade com os princípios da proporcionalidade e da razoabilidade. Recursos a que se nega seguimento” (TJERJ, Apelação Cível 0001387-41.2011.8.19.0202, rel. Des. Marco Antonio Ibrahim, j. 12-9-2011).

“Apelação cível — Direito do consumidor — Compra de aparelho celular realizada pela internet — Solidariedade entre o *site* de compra *online* e a empresa prestadora de serviço de intermediação comercial por meio eletrônico quanto à finalização da transação — Não entrega do produto — Responsabilidade solidária de todos que integram a ‘cadeia de fornecimento’ — Risco do empreendimento — Circunstância em que o autor, até a presente data, não recebeu a restituição — Situação que desborda do mero descumprimento contratual, tornando inaplicável a Súmula 75 do TJRJ. Frustração da legítima expectativa do consumidor reforma parcial da sentença (...)” (TJRJ, 4ª Câm. Cív., Apelação Cível 2193188-70.2011.8.19.0021, rel. Des. Marcelo Lima Buhatem, j. 26-8-2011).

“Ação indenizatória. Compra realizada através de *site* na internet. Cancelamento unilateral. Produto divulgado. Caráter vinculativo. Princípio da confiança. Dano moral configurado. *Quantum* fixado em observância aos princípios da razoabilidade e proporcionalidade. Decisão monocrática com fulcro no art. 557, *caput*, do CPC, que nega seguimento aos recursos. A legislação consumerista vinculou o fornecedor àquilo que por ele é ofertado, protegendo, dessa forma, o consumidor. A ré deveria ter verificado o estoque ou a possibilidade de reposição do produto antes de oferecê-lo ao consumidor, o que não ocorreu na hipótese” (TJRJ, Apelação Cível 0151516-84.2008.8.19.0001, rel. Des. Vera Maria Soares Van Hombbeeck, j. 6-4-2011).

16. De acordo com a redação publicada no Diário da Câmara dos Deputados de 27 de setembro de 2001, às p. 46310 a 46317, do Substitutivo ao Projeto de Lei n. 4.906, art. 30: “Aplicam-se ao comércio eletrônico as normas de defesa e proteção do consumidor vigentes no País”.

17. No caso de relações comerciais entre fornecedor e consumidor de nacionalidades distintas, qual seria a legislação aplicável? O Código Civil entende aplicável a lei do domicílio ou da sede do fornecedor, enquanto o Código de Defesa do Consumidor determina que o fornecedor teria de se adaptar às diversas legislações de todos os lugares onde estivesse o consumidor, o que no ambiente da Internet significa, de fato, o mundo todo. Talvez uma solução conveniente seria adotar a lei do fornecedor, mas, quando essa sede fosse usada como artifício para burlar a proteção do consumidor, adotar-se-ia como regra a lei do consumidor.

15. Projeto de Lei n.1.232/2011. Jurisprudências:

rios, um termo que preveja a possibilidade de arbitragem e, num ambiente em que os *links* e parcerias entre várias empresas são inúmeros, que conheça bem seus parceiros. A segurança da transação virtual também depende de informações sobre o tipo de criptografia utilizada e sobre a existência ou não de seguro para a operação eletrônica.

No entanto, uma das questões mais importantes é a que envolve o pagamento. Por exemplo, quando faço um pedido por telefone, fico tranquilo porque sei que vou receber minha mercadoria, efetuar o pagamento e receber a nota fiscal. Na Internet existe a possibilidade técnica do envio de recibo de pagamento virtualmente — isso já acontece nos registros de domínio e no caso de pagamentos bancários via rede. O pagamento contra a apresentação da nota fiscal¹⁸, seja virtual, seja na entrega, é que permite a execução das obrigações de ambas as partes, já que não se consubstancia a compra e venda sem que tenha sido entregue a mercadoria e realizado o pagamento do preço acordado, no prazo e local estabelecidos entre as partes.

As responsabilidades pelo armazenamento adequado, transporte e entrega da mercadoria também podem funcionar como no mundo real. Aquele que faz o contato direto com o consumidor final é sempre o responsável por resolver problemas com a mercadoria vendida, como entregas não feitas dentro do prazo, itens com defeito de fábrica ou causados por armazenamento incorreto. Aplicam-se aqui os princípios de corresponsabilidade¹⁹ do vendedor, resguardados os direitos de regresso²⁰ destes contra os fabricantes, os responsáveis pelo estoque ou as transportadoras. Mais uma vez, a informação surge como item

18. Questão importante a ser lembrada é a referente à nota fiscal. Algumas empresas sobretudo no que toca à prestação de serviços, não estão fornecendo as respectivas notas fiscais, situação esta que gera insegurança e inibe as possíveis compras de valores mais elevados. Se é verdade que a carga tributária no Brasil é muito elevada e pode inviabilizar a implantação do comércio eletrônico pelas pequenas empresas, também é verdade que a Internet não pode ser encarada como um caixa dois, abrigando atividades à margem da legalidade. Uma solução que incentivaria o comércio eletrônico e mesmo assim não desprotegeria o consumidor seria que o Governo tratasse a Internet como uma zona de livre comércio, concedendo isenções fiscais aos atos de comércio realizados em ambiente eletrônico para as empresas regularmente cadastradas de modo a fomentar as transações comerciais.

19. A responsabilidade solidária do fornecedor em face do consumidor pelos vícios do objeto está presente em diversos artigos do Código de Defesa do Consumidor. Os principais são os arts. 12, 14, 18, 19 e 20.

20. O direito de regresso está assegurado no parágrafo único do art. 13 da Lei n. 8.078, de 1990, que dispõe sobre a proteção do consumidor e dá outras providências: “Parágrafo único. Aquele que efetivar o pagamento ao prejudicado poderá exercer o direito de regresso contra os demais responsáveis, segundo sua participação na causação do evento danoso”.

fundamental: deixar claro quem são os seus parceiros traz credibilidade perante os consumidores e contribui para solucionar conflitos.

Entendemos que os contratos entre os participantes da cadeia de venda também devem prever algumas situações. Se uma empresa se compromete a fornecer equipamentos para serem vendidos por um *site* de *e-commerce*, deve saber a que países esse *site* pretende vender seus produtos, para saber se poderá dar assistência técnica²¹ nesses territórios. Se o *site* não tiver uma política clara a respeito, é importante que seja definida contratualmente a não responsabilidade do fornecedor por problemas ocorridos em territórios que este não possa atender. O mesmo vale para empresas de transporte: elas têm de saber qual o período de entrega dos produtos que um *site* de vendas promete a seus consumidores, para saber até que ponto pode cumpri-los e quais os limites físicos de sua atuação. Assumir prazos de entrega de até vinte e quatro horas normalmente significa a exigência de estoque *in house*.

Não podemos esquecer da modalidade de *Shopping Virtual* que nasceu com a Internet e representa o modelo existente no mundo real em que há uma multiplicidade de lojas em regime de condomínio para dar aos clientes mais comodidade, lazer e segurança. Os *shopping centers* virtuais geram também situações interessantes. Nenhum consumidor vai procurar a administração de um *shopping center* do mundo real para reclamar de um produto adquirido em uma de suas lojas — ele irá direto na loja que efetuou a venda. Mas os *shopping centers* virtuais deslocam a atenção dos consumidores para a marca desse *shopping*, não para as outras marcas contidas nele, tornando-o o centro das reclamações e ações do consumidor.

Devemos ressaltar que há duas situações distintas que têm diferentes consequências em termos jurídicos: 1) Quando a loja está em um *link* com o *shopping* virtual e o internauta é levado ao espaço da loja quando clica no *link*; 2) Quando a loja é um espaço dentro do domínio virtual do *shopping* como no caso em que se abre um *pop-up* ou *hotsite*²². Nesta segunda hipótese, um *banner* não me reporta à loja, mas me mantém em um *pop-up* que segue a programa-

21. O dever de prestar assistência técnica está contido no art. 32 do Código de Defesa do Consumidor.

22. *Pop-up* e *Hotsite* são modalidades de interface gráfica elaboradas com fins e tecnologias distintas. O *Pop-up* costuma se apresentar como uma janela complementar ao *site* principal com o fim de apresentar informações, avisos e muitas vezes publicidade, enquanto o *Hotsite* nada mais é que um *site* de estrutura simplificada e de menor porte, normalmente desenvolvido para suportar uma campanha publicitária de produtos ou serviços tendo, portanto, um período de vida curto.

ção visual do provedor (no caso, o *shopping* virtual), que para este está gerando *page-views* e, portanto, torna-o responsável pela transação. Então, a arquitetura do *site* tem de ser pensada em conjunto com sua parte jurídica: se uma empresa vai utilizar-se dos mecanismos de *pop-up*, tem de deixar bem claro quem serão os responsáveis pelo que ocorre ali.

Em Direito, como sabemos, não existe um ato que não tenha um responsável — o sujeito só se exime de uma responsabilidade se outro a assumir. Portanto, dependendo da estratégia jurídica e da arquitetura do *site* para conquistar *page-views*, pode-se estar criando uma situação de corresponsabilidade desnecessária e até colocando em risco a imagem da marca junto ao consumidor. Por isso é essencial o conhecimento do Direito Digital, tanto sob o aspecto jurídico como principalmente sob o aspecto estratégico e tecnológico. Será cada vez mais recomendável trazer o advogado para o processo inicial de concepção do próprio *website*, para que a arquitetura esteja construída dentro de uma estratégia não só comercial como também jurídica.

Devemos ressaltar, por oportuno, outra modalidade de comércio eletrônico caracterizada por serem empresas ambas as partes e não haver consumidor final na transação comercial. Esse comércio entre empresas, o chamado *Business-to-Business*, ou somente B2B, não se enquadra no Código de Defesa do Consumidor, que só se aplica ao consumidor final de um produto. Nesse mercado B2B concentra-se o maior volume de transações da Internet: os metamercados, como são chamados os pontos de encontro virtuais entre empresas compradoras e fornecedoras, que acarretam grande redução de custos operacionais para seus participantes. Funcionam como pregões privados: muitas vezes o *site* pode ser equiparado à figura do corretor.

A questão fundamental que se coloca diz respeito à responsabilidade. Quem é responsável por problemas²³ ocorridos nesse âmbito? Depende da

23. É interessante observar que, se, por um lado, o *site* B2B traz consigo a ideia de transparência, agilidade e eficiência nas informações, por outro lado, gera práticas tendentes à cartelização. A Lei n. 8.884, de 11 de junho de 1994, que dispõe sobre a prevenção e a repressão às infrações contra a ordem econômica e dá outras providências, arrola em seu art. 21 condutas que seriam características de cartel, entre elas: fixação de preços e condições de venda (inc. I), promoção de condição-comercial uniforme ou concertada entre os concorrentes (inc. II), divisão de mercados (inc. III), conluio na concorrência pública ou administrativa (inc. VIII) e regulação de mercados (inc. X). No caso da Covisint, *joint venture* constituída pelas empresas Ford, General Motors, DaimlerChrysler e Renault/Nissan, acredita-se que, por meio de seu *site* B2B, criado para compra de peças e partes automotivas, a Covisint estaria forçando os fornecedores de peças a negociar apenas pelo *site* e que este procedimento proporcionaria a constituição de práticas comerciais uniformes ou concertadas entre os concorrentes. Apesar de a notória vantagem do comércio nos *sites* B2B ser a redução dos custos operacionais, sabemos que não é prática dos cartéis repassar para os consumidores os ganhos com eficiência e sim maximizar seus lucros.

arquitetura do *website*. Se a transação puder ser fechada *online*, o *site* provavelmente será corresponsável pelas transações. E esse é o caso mais comum nos metamercados: a eficiência da Internet baseia-se em sua capacidade de concentrar toda a operação virtualmente — minutas de contrato *online*, recibos das transações etc. Um ambiente que não tenha essa capacidade seria apenas uma vitrina, uma feira de exposições, não uma feira de vendas.

Os contratos entre os participantes do comércio B2B devem ter cláusulas especiais e específicas, no âmbito de mercado *online*, devendo observar: prazo, responsabilidade por etapa, citação dos parceiros terceirizados, seguro, empresa certificadora da operação, endereços eletrônicos de compra e venda autorizados (o fornecedor tem de saber em que espaços virtuais a ponta de venda está atuando). Na ponta da entrega, a empresa deve buscar minimizar os riscos de falha, com o consequente impacto negativo para a marca.

Os serviços de *call-center*, normalmente terceirizados, são uma parte importante na economia das empresas que operam virtualmente. Os contatos, nos casos de *call-centers* virtuais, serão sempre eletrônicos (seja por *e-mail*, *chat* ou *video streaming*); podem, portanto, ocorrer a qualquer momento e vir de qualquer parte do mundo. É importante informar claramente ao usuário o horário de funcionamento do *call-center*, seus meios de acesso e o tempo de retorno; enfim, toda a rotina-padrão de operações de atendimento ao consumidor.

As companhias que estão aderindo ao comércio eletrônico têm encontrado dificuldades não somente em implantar novas tecnologias, mas também na integração entre as estruturas de retaguarda e as facilidades da *web*. Muitas vezes, a implementação de “estratégias de *e-commerce*” implica alterações profundas nas empresas. Todos os departamentos afetados devem estar envolvidos na operação. Especialistas em concorrência nos negócios *online* defendem a necessidade de táticas para auxiliar as companhias a sobreviverem com sucesso no futuro. Para entender como colaborar e interoperar neste ambiente é importante ter, além de estratégia, a abordagem tática. Muito desta abordagem cabe aos advogados digitais na correta assistência dos negócios de seus clientes.

8.4. Consumidor *online* e o CDC à luz do Direito Digital

O consumidor atual já é digital. De certo modo, mesmo não realizando a transação através da Internet, isso não quer dizer que a forma de coletar informações sobre bens e serviços já não ocorra de modo maciço pela *web*. Ou seja, desde o advento do Código de Defesa do Consumidor brasileiro (CDC), em

1990, estamos assistindo ao amadurecimento das relações de consumo, e do próprio consumidor.

Logo, vemos que o consumidor mudou, está mais informado, utiliza ambientes remotos de relacionamento (telefone, celular, *messenger*, *chat*, comunidades, redes sociais, *e-mail*, internet); tem mais conhecimento sobre seus direitos; quer tudo para ontem (síndrome da vida em tempo real); negocia seu poder de “clique” (o concorrente está a um clique de distância); quer atendimento personalizado, mas sem exageros na comunicação (invasão de privacidade).

Além disso, a própria Internet hoje serve não apenas como canal de informação, mas como de denúncia: <www.reclameaqui.com.br>, <www.ebit.com.br>, <www.idec.gov.br>, <www.portaldoconsumidor.gov.br>, entre outros.

As regras previstas pelo Código do Consumidor aplicam-se tanto ao mundo real como ao virtual. No ambiente eletrônico, porém, pelas partes estarem de modo não presencial, não haver manuseio de produto, ter a possibilidade de distorções de tamanho, cor e outras características no uso de imagens em *sites* de comércio eletrônico, este tipo de compra precisa ser realizado com mais cautela.

Há informações essenciais a que o consumidor precisa estar atento, para não ter problemas após ter efetivado a contratação. Entre elas, devemos destacar os dados corretos sobre o estabelecimento comercial, já que também na Internet há uma presença grande de lojas que não possuem registro legal, que estão atuando de modo irregular, e, pela promessa de oferta de preço mais barato, o consumidor acaba sendo atraído para a compra, mas corre o risco de não receber o produto e não saber nem para quem endereçar sua reclamação ou ajuizar a ação judicial.

Em análise geral, a Lei n. 8.078/90, que instituiu o Código de Proteção e Defesa do Consumidor, tem princípios e artigos válidos inclusive para as relações eletrônicas e não presenciais, seja na Internet, seja no celular, ou em qualquer outro meio que se invente:

a) O reconhecimento dos Direitos Difusos e Coletivos nas relações de Consumo.

b) A definição de Consumidor — art. 2º²⁴ (inclusive já há decisões demonstrando situações de compra de *software* por empresa, na qual ela configu-

24. CDC, art. 2º: “Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.

Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo”.

raria como consumidor final, portanto com todas as proteções e garantias dadas pelo CDC²⁵.

c) Imputação da responsabilidade direta e de forma objetiva ao fornecedor independentemente do vínculo contratual. Antes do CDC havia dificuldade de imputação de responsabilidade ao fornecedor devido ao princípio do *pacta sunt servanda* (os contratos devem ser cumpridos), bem como dificuldade de prova de dano e de nexo causal — arts. 6º, 12 e outros²⁶.

d) O fabricante, vendedor ou prestador de serviços tem o dever de informar ao consumidor todas as características do produto ou serviço oferecido no mercado.

e) A propaganda tem força vinculante, integra o contrato e obriga o anunciante ao cumprimento de todas as promessas anunciadas, inclusive quanto ao preço, se mencionado.

25. Jurisprudências nesse sentido:

Acórdão 1 — Tribunal de Alçada de Minas Gerais — Acórdão: 0399930-2 Apelação (Cv) Cível Ano: 2003 — Segunda Câmara Cível. “Ementa: AÇÃO DE INDENIZAÇÃO — AQUISIÇÃO DE PROGRAMA DE *SOFTWARE* — ESTABELECIMENTO DE ENSINO — RELAÇÃO DE CONSUMO — VÍCIO NO PRODUTO — DECADÊNCIA — RESTITUIÇÃO DO PREÇO PAGO — PERDAS E DANOS NÃO COMPROVADOS — INADMISSIBILIDADE — APELO ADESIVO — AUSÊNCIA DE SUCUMBÊNCIA RECÍPROCA — NÃO CONHECIMENTO. — A circunstância de ser pessoa jurídica não pode afastar a relação de consumo, uma vez que a instituição de ensino não é mera intermediária ou insumidora do programa de *software* adquirido, mas, sim, destinatária final que exaure a utilidade do bem. (...)”.

Acórdão 2 — Tribunal de Justiça do Paraná. Acórdão: APELAÇÃO CÍVEL N. 0408404-8 (...) Da decisão em audiência (...), que acolheu a aplicação do código de defesa do consumidor, foi interposto agravo de instrumento pela apelante, o qual foi rejeitado pelo juízo *ad quem*, às fls. (...). Cuida-se de indenização por dano moral, porque a apelada, em data de 18 de maio de 2000, comprou um programa de computador da apelante, sendo que o mesmo em razão do funcionamento defeituoso causou uma série de transtornos, abalando a reputação da apelada diante de seus clientes. Da aplicação do CDC. Na espécie aplica-se o CDC, haja vista que além do agravo que discutira a matéria ter sido rejeitado, inegável a relação de consumo, dada a incidência dos artigos 2º e 3º, do referido diploma legal, bem como o produto comprado, se não fosse objeto de sérios problemas, seria utilizado pela apelada como destinatária final. (...) Presidiu o julgamento o Excelentíssimo Senhor Desembargador TUFU MARON FILHO. Curitiba, 10 de Maio de 2007 A. I. Reinaldin — Relator Substituto de 2º Grau (...)

26. Art. 6º, VIII — “a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências”.

Art. 12 — “O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos”.

f) Se a oferta ou venda for por telefone ou reembolso postal, o consumidor terá sete dias para desistir da compra, com direito à devolução das quantias eventualmente pagas. Neste item, há situações em que na compra e venda online, pelo e-commerce, também se aplica a mesma regra.

g) Proteção contra práticas abusivas contra o consumidor — prevista pelo art. 39²⁷.

h) Responder pelos danos patrimoniais e morais que causar. Esta proteção é de fundamental importância, especialmente na Internet, com a facilidade de usos de dados dos consumidores²⁸.

27. “Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas:

I — condicionar o fornecimento de produto ou de serviço ao fornecimento de outro produto ou serviço, bem como, sem justa causa, a limites quantitativos;

II — recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes;

III — enviar ou entregar ao consumidor, sem solicitação prévia, qualquer produto, ou fornecer qualquer serviço;

IV — prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços;

V — exigir do consumidor vantagem manifestamente excessiva;

VI — executar serviços sem a prévia elaboração de orçamento e autorização expressa do consumidor, ressalvadas as decorrentes de práticas anteriores entre as partes;

VII — repassar informação depreciativa, referente a ato praticado pelo consumidor no exercício de seus direitos;

VIII — colocar, no mercado de consumo, qualquer produto ou serviço em desacordo com as normas expedidas pelos órgãos oficiais competentes, ou, se normas específicas não existirem, pela Associação Brasileira de Normas Técnicas ou outra entidade credenciada pelo Conselho Nacional de Metrologia, Normalização e Qualidade Industrial — CONMETRO;

IX — recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais;

X — elevar sem justa causa o preço de produtos ou serviços;

XI — (dispositivo incorporado pela MP n. 1.890-67-1999, transformado em inciso XIII, quando da conversão na Lei n. 9.870-1999).

XII — deixar de estipular prazo para o cumprimento de sua obrigação ou deixar a fixação de seu termo inicial a seu exclusivo critério.

XIII — aplicar fórmula ou índice de reajuste diverso do legal ou contratualmente estabelecido. (Acrescentado pela Lei n. 9.870-1999)”.
28. Jurisprudências nesse sentido:

Acórdão 1 — Tribunal de Alçada do Paraná — Nona Câmara Cível — “CONTRATO DE IMPLANTAÇÃO DE SISTEMA DE SOFTWARE. INDENIZAÇÃO. PREJUÍZO DE EMPRESA ADQUIRENTE. DANOS MATERIAIS E MORAIS. CÓDIGO DE DEFESA DO CONSUMIDOR. APLICABILIDADE. VALOR FIXADO. LIMITE DA

i) Permitir apenas maiores em seu estabelecimento se explorar comercialmente jogos ou apostas. Essa questão, junto com o Estatuto da Criança e do Adolescente, motivou a criação de algumas regras específicas para Lan Houses, como já previsto na Lei Estadual Paulista n. 12.228/2006²⁹, entre outras.

INICIAL. DANO MORAL INDEVIDO. MAJORAÇÃO PREJUDICADA. HONORÁRIOS ADVOCATÍCIOS. FIXAÇÃO ENTRE O MÍNIMO E O MÁXIMO PERMITIDO.

1. Presentes a adequação fática e a definição de consumidor e fornecedor dispostos na lei, aplicam-se ao contrato as regras do Código de Defesa do Consumidor.

2. ‘Aquele que comercializar programa de computador, quer seja titular dos direitos do programa, quer seja titular dos direitos de comercialização, fica obrigado, no território nacional, durante o prazo de validade técnica da respectiva versão, a assegurar aos respectivos usuários a prestação de serviços técnicos complementares relativos ao adequado funcionamento do programa, consideradas as suas especificações’ (art. 8º da Lei 9.609/98).”

Acórdão 2 — Tribunal de Justiça do Rio de Janeiro, Décima Primeira Câmara Cível

APELAÇÃO CÍVEL N. 2007.001.06788 (...) A instituição bancária/ré permitiu que terceiro, utilizando do convênio firmado entre ela e uma empresa do ramo musical, realizasse compras através de débito automático na conta corrente do autor. Note-se que, mesmo diante das facilidades existentes no mercado de consumo, como a aquisição de produtos via telefone ou INTERNET, não se pode olvidar das cautelas pertinentes, a fim de impedir que outra pessoa faça uso dos dados pessoais do correntista para ocasionar lesão patrimonial. Destarte, não é admissível que as empresas de grande porte, que devem se municiar contra fraudes, resolvam atribuir culpa a terceiros com o objetivo de deixar o dito pelo não dito. Assim, tais circunstâncias não podem ser consideradas meros aborrecimentos, em virtude do que faz jus o autor à indenização por danos morais, fixada no valor de R\$ 12.000,00 (doze mil reais), corrigidos monetariamente e acrescido de juros de mora de 1% (um por cento) ao mês, a contar da citação, conforme a sentença, eis que reproduz a justa reparação do dano, atendendo os princípios da razoabilidade e proporcionalidade. Recurso conhecido e improvido. Rio de Janeiro, 16 de maio de 2007. DESEMBARGADOR CLAUDIO DE MELLO TAVARES. Presidente/Relator

29. Lei estadual n. 12.228/2006 — Estado de São Paulo — Cibercafés e Lan houses

Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências.

O Governador do Estado de São Paulo:

Faço saber que a Assembleia Legislativa decreta e eu promulgo a seguinte lei:

Artigo 1º São regidos por esta lei os estabelecimentos comerciais instalados no Estado de São Paulo que ofertam a locação de computadores e máquinas para acesso à Internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como “lan houses”, cibercafés e “cyber offices”, entre outros.

Artigo 2º Os estabelecimentos de que trata esta lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:

I — nome completo;

II — data de nascimento;

III — endereço completo;

IV — telefone;

V — número de documento de identidade.

§ 1º O responsável pelo estabelecimento deverá exigir dos interessados a exibição de documento de identidade, no ato de seu cadastramento e sempre que forem fazer uso de computador ou máquina.

§ 2º O estabelecimento deverá registrar a hora inicial e final de cada acesso, com a identificação do usuário e do equipamento por ele utilizado.

§ 3º Os estabelecimentos não permitirão o uso dos computadores ou máquinas:

1. a pessoas que não fornecerem os dados previstos neste artigo, ou o fizerem de forma incompleta;

2. a pessoas que não portarem documento de identidade, ou se negarem a exibi-lo.

§ 4º As informações e o registro previstos neste artigo deverão ser mantidos por, no mínimo, 60 (sessenta) meses.

§ 5º Os dados poderão ser armazenados em meio eletrônico.

§ 6º O fornecimento dos dados cadastrais e demais informações de que trata este artigo só poderá ser feito mediante ordem ou autorização judicial.

§ 7º Excetuada a hipótese prevista no § 6º, é vedada a divulgação dos dados cadastrais e demais informações de que trata este artigo, salvo se houver expressa autorização do usuário.

Artigo 3º É vedado aos estabelecimentos de que trata esta lei:

I — permitir o ingresso de pessoas menores de 12 (doze) anos sem o acompanhamento de, pelo menos, um de seus pais ou de responsável legal devidamente identificado;

II — permitir a entrada de adolescentes de 12 (doze) a 16 (dezesseis) anos sem autorização por escrito de, pelo menos, um de seus pais ou de responsável legal;

III — permitir a permanência de menores de 18 (dezoito) anos após a meia-noite, salvo se com autorização por escrito de, pelo menos, um de seus pais ou de responsável legal.

Parágrafo único. Além dos dados previstos nos incisos I a V do artigo 2º, o usuário menor de 18 (dezoito) anos deverá informar os seguintes:

1. filiação;

2. nome da escola em que estuda e horário (turno) das aulas.

Artigo 4º Os estabelecimentos de que trata esta lei deverão:

I — expor em local visível lista de todos os serviços e jogos disponíveis, com um breve resumo sobre os mesmos e a respectiva classificação etária, observada a disciplina do Ministério da Justiça sobre a matéria;

II — ter ambiente saudável e iluminação adequada;

III — ser dotados de móveis e equipamentos ergonômicos e adaptáveis a todos os tipos físicos;

IV — ser adaptados para possibilitar acesso a portadores de deficiência física;

V — tomar as medidas necessárias a fim de impedir que menores de idade utilizem contínua e ininterruptamente os equipamentos por período superior a 3 (três) horas, devendo haver um intervalo mínimo de 30 (trinta) minutos entre os períodos de uso;

VI — regular o volume dos equipamentos de forma a se adequar às características peculiares e em desenvolvimento dos menores de idade.

Artigo 5º São proibidos:

I — a venda e o consumo de bebidas alcoólicas;

II — a venda e o consumo de cigarros e congêneres;

III — a utilização de jogos ou a promoção de campeonatos que envolvam prêmios em dinheiro.

j) Fazer orçamento nos termos do art. 40, §§ 1º a 3º.

k) Ampliação da responsabilidade solidária, com garantia de direito de regresso, o que na Internet ocorre com frequência, principalmente pelo grau de interdependência dos negócios — art. 13³⁰. Sendo que em situações em que o fornecedor possa fazer prova da culpa exclusiva do consumidor ou de terceiro, então poderia afastar sua responsabilidade. A aplicação do art. 14 tem sido debatida no sentido de limites de responsabilidade, especialmente quando envolver danos causados por negligência do cliente, como em situações de uso indevido de senha no Internet Banking, entre outros³¹.

Artigo 6º A inobservância do disposto nesta lei sujeitará o infrator às seguintes penalidades:

I — multa, no valor de R\$ 3.000,00 (três mil reais) a R\$ 10.000,00 (dez mil reais), de acordo com a gravidade da infração, conforme critérios a serem definidos em regulamento;

II — em caso de reincidência, cumulativamente com a multa, suspensão das atividades ou fechamento definitivo do estabelecimento, conforme a gravidade da infração.

§ 1º Na reincidência, a multa será aplicada em dobro.

§ 2º Os valores previstos no inciso I serão atualizados anualmente, pelos índices oficiais.

Artigo 7º O Poder Executivo regulamentará esta Lei, especialmente quanto à atribuição para fiscalizar seu cumprimento e impor as penalidades a que se refere o artigo 6º.

Artigo 8º Esta Lei entra em vigor após decorridos 30 (trinta) dias de sua publicação oficial.

Palácio dos Bandeirantes, aos 11 de janeiro de 2006.

GERALDO ALCKMIN

Hélio Silva Júnior

Secretário da Justiça e da Defesa da Cidadania

Saulo de Castro Abreu Filho

Secretário da Segurança Pública

Arnaldo Madeira

Secretário-Chefe da Casa Civil

30. "Art. 13. O comerciante é igualmente responsável, nos termos do artigo anterior, quando:

I — o fabricante, o construtor, o produtor ou o importador não puderem ser identificados;

II — o produto for fornecido sem identificação clara do seu fabricante, produtor, construtor ou importador;

III — não conservar adequadamente os produtos perecíveis.

Parágrafo único. Aquele que efetivar o pagamento ao prejudicado poderá exercer o direito de regresso contra os demais responsáveis, segundo sua participação na causação do evento danoso."

31. Art. 14, § 3º, II, do CDC: "§ 3º O fornecedor de serviços só não será responsabilizado quando provar: (...) II — a culpa exclusiva do consumidor ou de terceiro".

l) Possibilidade de cancelar serviços de prestação continuada, como já foi previsto pela Lei paulista n. 12.281/2006³².

m) A proteção de bancos de dados de consumidores e a questão de privacidade, hoje muito discutida no âmbito da Internet, em que se aplicam os artigos do CDC³³, bem como o art. 5º da Constituição Federal.

n) Inversão do ônus da prova em favorecimento ao consumidor³⁴. Esta situação gera uma preocupação cada vez maior dos fornecedores e lojas virtuais em fazer a guarda adequada das provas eletrônicas, uma vez que caberá a elas provar se determinado fato ocorreu ou não, inclusive se é situação até mesmo de autofraude. Esta guarda adequada é essencial para proteção legal da empresa em relações de consumo sujeitas ao CDC. Isso porque muitas vezes, sem preparar o terreno antecipadamente, a empresa pode ficar sem defesa!

Da mesma forma que o Código de Defesa do Consumidor se aplica às compras reais, o direito de arrependimento também é aplicável para as compras

32. Lei Paulista n. 12.281, de 2006:

As prestações de serviços continuadas — No dia 22 de fevereiro de 2006 entrou em vigor, no estado de São Paulo, a Lei n. 12.281. Os consumidores paulistas têm motivos para festejar a atenção que lhes deu o legislador com os direitos ali consagrados. É que, muito embora o Código de Defesa do Consumidor — Lei federal n. 8.078/90, já assegure ao consumidor que o fornecedor não poderá concluir, alterar ou rescindir o contrato de maneira unilateral, ou exigir obrigações consideradas iníquas, abusivas, ou que coloquem o consumidor em desvantagem exagerada (art. 51), a lei paulista veio dar tratamento específico aos contratos de prestação de serviços contínuos.

São aqueles contratos denominados pela Professora Cláudia Lima Marques Contratos cativos de longa duração, já que envolvem prestações de trato sucessivo, que se prolongam no tempo. Característica: *assegurar aos consumidores a liberdade de solicitar o cancelamento do serviço pelos mesmos meios com que os contratou. Torna também obrigatório que o provedor de Internet facilite o cancelamento do serviço por telefone ou Correio.* O Código de Defesa do Consumidor considera tal prática abusiva, o que enseja aplicação de severa sanção, que vai de duzentas a três milhões de UFIRs. Da mesma forma, a Lei paulista n. 12.281/2006 determina que sejam aplicadas as sanções previstas no art. 56 do CDC. Mas, atenção: *não existe na festejada lei paulista a renovação automática dos contratos que tenham prazo determinado.* Não foi essa a intenção do legislador paulista, *nem poderá o fornecedor transferir para o consumidor o ônus de cancelar, expressamente, os contratos que tenham prazo determinado.*

33. CDC, art. 43 (sobre bancos de dados):

(i) os *cadastros e dados de consumidores* devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão;

(ii) a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor;

(iii) direito do consumidor de providenciar *correção de seus dados* (5 dias para o arquivista comunicar a alteração).

34. Art. 6º, VIII — “a *facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências*”.

realizadas em ambiente virtual, nos termos do art. 49 do texto legal. O direito de arrependimento nada mais é do que o consumidor que desiste de uma compra, feita *online*, isto é, fora do estabelecimento comercial³⁵, pode fazê-lo sem qualquer ônus e dentro do prazo de, pelo menos, sete dias.

Os serviços financeiros são entendidos como sujeitos também ao CDC, conforme decisão proferida pelo Supremo Tribunal Federal. Essa matéria era objeto de certa polêmica no Brasil, e com a tendência da evolução dos serviços bancários, cada vez mais eletrônicos, ela se torna de fundamental importância³⁶. A boa prática tem sido a elaboração de uma Política de Privacidade, que deve estar clara e objetiva no *website*, no momento da coleta dos dados, com barreira de navegação e guarda do “log” de ciência, para evitar que a empresa venha a ser questionada sobre a legitimidade de uso dos dados dos clientes.

Sendo assim, há uma série de regras válidas para o ambiente virtual, em que ele facilita a documentação da relação. Um *e-mail* enviado ao SAC *online* da empresa não respondido já é evidência de omissão. Os meios de comunicação eletrônica têm exigido que tanto fornecedores como consumidores façam uso de seus direitos e obrigações de modo mais responsável.

Cabe à empresa definir de modo claro a relação através da Internet. Afinal, seu consumidor pode estar acessando de qualquer lugar, e em uma discus-

35. BRUNO, Fabio de Barros. *E-Commerce e o Direito de Arrependimento*. Trabalho publicado nos Anais do XVIII Congresso Nacional do CONPEDI, realizado em SP nos dias 4 a 7 de novembro de 2009. Disponível em: <http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2335.pdf>. Acesso em: 3-10-2011.

36. Nesse sentido ver a Ação Direta de Inconstitucionalidade n. 2.591, conforme abaixo:
AÇÃO DIRETA DE INCONSTITUCIONALIDADE (Med. Liminar) 2.591 — 1

Requerente: CONFEDERAÇÃO NACIONAL DO SISTEMA FINANCEIRO — CONSIF (CF 103, 0IX) Requerido: PRESIDENTE DA REPÚBLICA CONGRESSO NACIONAL

Dispositivo Legal Questionado:

Art. 3º, § 2º, da Lei n. 8.078, de 11 de setembro de 1990, na expressão “inclusive as de natureza bancária financeira de crédito e securitária”. Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a Proteção do Consumidor e dá outras providências. Art. 3º Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividades de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços. (...) § 2º Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

Resultado Final: Improcedente.

são jurídica, na grande maioria dos casos, irá prevalecer o ordenamento jurídico do domicílio do consumidor.

8.5. O *e-Business* para as Classes C e D — baixa renda

O varejo virtual continua com altos índices de crescimento. Quer seja pela falta de tempo, pela comodidade, pela oferta de melhores preços, comprar pela Internet está se tornando rotina dos brasileiros. Assim como crescem os consumidores *online*, também crescem os riscos relacionados a questões de segurança. Como ficam os limites jurídicos de responsabilidades e obrigações quando se trata de uma loja virtual?

Com a massificação de uso de meios eletrônicos nas operações de pagamento, bem como da Internet para transacionar junto ao banco ou à loja, o próximo desafio é a mobilidade, trazida por um novo perfil de usuário digital, que está nas Classes C e D. Afinal, apesar de muitos não terem computador em casa, nem banda larga, a maioria tem celular.

Logo, fica a questão: como gerar prova de autoria, de identidade, para aproveitar o potencial de negócios pela via eletrônica-móvel junto a este público que possui um volume expressivo. Mesmo o varejo que está há anos na *web*, ou quem deixou para entrar só agora, deve refletir em como tirar proveito com o menor risco jurídico, uma vez que há uma tendência de a Justiça brasileira estabelecer a hipossuficiência compulsória, ou seja, se é consumidor, com baixo nível de escolaridade, com baixa renda, então não sabia o que estava fazendo, ainda mais quando se faz uso de recursos tecnológicos.

Neste cenário, como fica a questão do uso do certificado digital com a migração para mobilidade? Seria uma solução viável? O certificado digital da ICP-Brasil não apenas permite uma “assinatura digital” como deve ser tratado pela Justiça com o mesmo valor legal de uma assinatura com firma reconhecida.

Em todas as relações transacionais há sempre um ônus de prova de autoria por parte do contratado do serviço, do prestador, cabendo a ele a conferência desta identidade no momento da contratação. Isso já é vivido como um verdadeiro pandemônio jurídico-financeiro nas operações de cartão de crédito ou de débito com ausência do mesmo (via telefone e Internet), que elevam a probabilidade de repúdio. Pois quando a relação é presencial, é óbvio que, se o estabelecimento não faz conferência da identificação do contratante, assume o risco. Não apenas há o criminoso como também é muito comum no Brasil a situação do consumidor oportunista, que se aproveita da inversão do ônus da prova para tentar não pagar pelo que comprou.

Como saber quem de fato está do outro lado da interface gráfica? Em termos jurídicos, deve ser gerada uma presunção legal, que é o que ocorre quando se determina que a identificação do usuário será uma senha única, individual, sigilosa, e que, em tese, só o usuário deveria ter conhecimento. O mesmo que ocorre com a personalidade da Pessoa Jurídica, que é uma invenção legal para determinar uma identidade que possa assumir obrigações e responsabilidades, e que representou uma grande inovação em sua época de criação.

O certificado digital da ICP-Brasil só vai se tornar uma ferramenta de proteção jurídica de verdade quando passar a ser obrigatório para declaração de imposto de renda de pessoas físicas. Mas cabe a quem pagar esta conta? Em princípio, sempre recai para o cidadão, visto que o mesmo tem de pagar para ter um passaporte, por exemplo, para trafegar nas vias internacionais-presenciais.

Não podemos apenas dar um celular, um acesso à Internet. Temos de conseguir garantir segurança jurídica das relações que ocorrem pelo meio digital. Ou seja, garantir que tudo isso esteja em conformidade legal e que as partes cumprirão com o combinado. Isso gera segurança para os negócios, segurança social. Devemos sim dar o próximo passo da mobilidade, massificar o uso dos canais eletrônicos, com o máximo de proteção às informações em todas as pontas. Do celular do cliente ao sistema da loja ou do banco, do computador do usuário ao provedor de acesso à Internet, da operadora de celular ao servidor de *mobile banking*, da área de TI da Empresa ao Fisco via SPED. Até quando vamos negar que a única coisa realmente importante é saber quem é quem dentro do ambiente eletrônico.

Afinal, a questão da segurança é considerada um risco do próprio negócio (art. 927 do Código Civil), ou uma parcela disso deve ser assumida pelo cliente (art. 14 do Código de Defesa do Consumidor)? E quando a questão envolve espionagem eletrônica, concorrência desleal, furto de bases de dados de clientes, como fazer? Nosso varejo virtual já está amadurecido com base nas melhores práticas de mercado e para atender ao Código de Defesa do Consumidor em vigor? Já podemos lançar voos mais altos com mobilidade total ou vamos repetir os mesmos erros da Internet no celular?

Não podem mais as empresas de varejo continuarem a circular informação de cliente por planilha de Excel, ou ter um *call-center* sem mínimos padrões de segurança. O *site* precisa ter um padrão aceitável de criptografia, bem como evitar que haja uma programação que facilite ataques do tipo *SQL Injection*. Tem sido comum lojas virtuais possuírem vulnerabilidades bem básicas, que podem ser exploradas por qualquer adolescente mal-intencionado ou mesmo por uma quadrilha interessada em pegar dados de cartão de crédito.

Segurança da Informação em loja virtual é uma necessidade de conformidade legal. Aplica-se tanto o Código de Defesa do Consumidor como o Código Civil, especialmente por causa da grande quantidade de parcerias operacionais que são estabelecidas com terceiros (fornecedores), sem os quais a loja virtual não funciona. Estão nesta categoria desde a empresa de hospedagem, de banco de dados, de entregas, para formalizar a transação com cartão de crédito, muitas vezes ainda uma financeira, pois há lojas que possuem cartão de crédito de marca própria, entre outros.

Periodicamente a loja deve fazer testes de vulnerabilidade para medir seu grau de segurança. Mas não adianta estar seguro para fora, e, dentro da loja, junto aos funcionários, ser comum um colaborador ou chefe passar a senha para outro. A senha é como a chave que abre uma porta para o patrimônio mais importante que está em dados. Estes dados, nas lojas, representam tanto operações, ou seja, seu uso indevido pode provocar uma fraude, com impactos financeiros e de reputação, como também representam o comportamento de seus clientes. Já acompanhamos um caso em que um ex-funcionário de uma loja virtual assediou um cliente em uma comunidade do Orkut, alegando, de forma ameaçadora, que sabia o que ele estava comprando na Internet, seu endereço, o nome da esposa e dos filhos.

Toda loja virtual deve ter um termo de uso adequado, que trate inclusive de política de troca e devolução. É recomendável, ainda, o uso de um carimbo do tempo, para determinar a hora legal da operação, a exposição de um relógio com data, hora, minuto e segundo no *site*, bem como uma política clara de privacidade. Além disso, os contratos de TI e Telecom, e seus respectivos Acordos de Nível de Serviço (SLAs) devem ser diferenciados para as lojas virtuais, já que a questão da indisponibilidade de serviços tem impacto diferente se tiver ocorrido em um dia qualquer ou às vésperas de um dia das mães, por exemplo, quando há um pico de venda, e a loja não pode ficar fora do ar em hipótese alguma. Não pode uma loja virtual ter um contrato padrão aplicável a outro tipo de negócio que o fornecedor de TI e Telecom atende, há necessidades, riscos e responsabilidades específicos.

A guarda das provas eletrônicas é essencial, ter um servidor de *logs* e guardar os dados completos de acessos, inclusive números de IP, pode fazer toda diferença se houver uma demanda judicial. Deve ser feita uma política de gestão documental com uma tabela de temporalidade, em que os dados que vêm do *site* devem ser guardados no mínimo por 12 meses. Principalmente porque é comum haver inversão de ônus da prova em situações que envolvem consumidor final. Segurança técnica e jurídica da informação para uma loja

virtual não é só uma questão de atender ou não as melhores práticas da ISO 27002, representa, na verdade, proteção do próprio negócio.

A loja virtual precisa ter informações claras e objetivas. Isso deve ser apresentado de forma fácil no *site*, com uso de termos e políticas, bem como por meio de um canal de contato eficiente (por *e-mail* ou telefone). Também é boa prática a apresentação de informações sobre número de CNPJ, endereço físico (não apenas o virtual), alvará de licença (informações mínimas de que a loja de fato existe legalmente e não é nem ilegal nem fantasma, sendo esta última muito comum para dar golpes nos consumidores desavisados que vão atrás só da oferta de preço mais baixo e não se preocupam em verificar se de fato a loja existe).

Além disso, a maior parte dos contratos eletrônicos são do tipo “adesão” (art. 54 do CDC). Logo, é fundamental que esses contratos sejam objetivos, claros, tenham descrito claramente todas as condições essenciais do produto/serviço, com detalhamento técnico quando necessário, bem como também apresentem regras claras sobre cancelamento, troca, devolução, desistência (art. 49, *caput* e parágrafo único). Cabe à empresa prestar as informações de forma certa, com guarda de ciência (ex.: guardar o *log* da tela com barreira de navegação, fazer envio automático do contrato para o *e-mail* cadastrado do cliente), e, do outro lado, cabe ao cliente ler o mesmo. Não caberá ao consumidor alegar que “viu mas não leu”. Deve-se ter muito cuidado com o uso de cláusulas que eximem responsabilidades (arts. 25, 28, 50, 51 do CDC).

Há situações corriqueiras em que não fica claro por parte da empresa como o cliente deve resolver o seu problema, tais como: a) um cliente que compra um produto e não sabe para onde mandar o mesmo para fazer a troca, pois a loja só tem domínio e *e-mail*, não tem endereço físico; b) o cliente que compra um *software*, faz *download*, e depois se o computador tem um problema de vírus e precisa reformatar o equipamento e não está claro na licença se ele pode receber novamente o *software* para mera reinstalação, já que não pode pegar do *backup*; c) ou ainda o estudante que contrata um curso a distância e durante a execução do mesmo adoece e quer saber se poderá fazer em outro momento ou receber o dinheiro de volta.

Em situação de dúvida, a lei vai proteger o consumidor, e interpretar que houve omissão ou má prestação de informação por parte do vendedor, o que faz com que assuma o risco e a responsabilidade pelo incidente (art. 47 do CDC). O consumidor deve ficar atento à questão da proteção dos seus dados (política de privacidade e uso de certificados de segurança são essen-

ciais). Para as lojas, aquela que é mais segura, por certo não vai só vender mais, com ticket médio maior, mas também terá seu cliente voltando mais vezes, fidelizado³⁷.

Concluindo, tanto para o varejo na Internet como para os negócios em mobilidade, que querem alcançar o cliente de qualquer lugar e em todo lugar, não será com uma mera senha de 4 dígitos (formato dos mais inseguros técnicos e juridicamente falando) que vamos conseguir isso, combatendo a fraude e aumentando a adesão. Quanto mais gente, mais oportunidades, e mais riscos, pois vivemos em rede, em uma grande comunidade digital na qual o comportamento de um gera consequências para todos. Enquanto não resolvemos esta questão, o fraudador, o estelionatário e o espertinho ficam com a maior parte do lucro.

37. Dicas para ter uma compra virtual com menos risco legal:

- verificar os dados cadastrais do domínio no *site* <www.registro.br> (para ver qual endereço, telefone, CNPJ e responsável que aparecem);
- fazer uma rápida busca na Internet para ver se o *site* está com alguma denúncia no Procon, Reclame Aqui, Comunidades, outros. Analisar estas informações com cautela, pois muitas vezes o problema já foi resolvido mas continua publicado;
- verificar se o *site* apresenta dados de telefone e endereço físico, além de *e-mail*;
- verificar se o *site* possui algum certificado de segurança;
- verificar se o *site* possui termos e políticas claras (compra e venda, termo de uso, troca ou devolução, cancelamento, privacidade, segurança, direitos autorais);
- verificar se no preço está incluso o frete;
- verificar se o *site* apresenta informações claras e completas sobre o produto/serviço, se a foto (imagem) corresponde à realidade ou é meramente ilustrativa;
- verificar se o *site* possui *tracking* do pedido (e se o cliente recebe o número para acompanhar);
- verificar se o *site* apresenta lista de parceiros para assistência técnica (quando aplicável);
- recomenda-se testar o *site* antes mandando um *e-mail* de dúvida e pedindo confirmar algumas informações. Se não for respondido, imagina se fosse uma reclamação;
- quando possível optar por um pagamento após entrega (que ocorre quando se paga com cartão de crédito) ou por pagamento contraentrega, evitando depósito direto em conta antecipado;
- deve-se guardar algumas evidências eletrônicas para apoiar em eventual investigação ou ação judicial (ex.: print das telas, *e-mails* trocados);
- em havendo problema, deve-se formalizar o vendedor (ciência do fornecedor) por meio de *e-mail* de reclamação ou contato pelo SAC (isso evita a decadência do direito, art. 26, § 2º, I, do CDC).

8.6. O Social-SAC nas Redes Sociais

Atualmente, verifica-se uma alta circulação de conteúdos, produtos e serviços na Internet. Mas o consumidor digital já prefere buscar informação sobre uma empresa ou sobre uma experiência de compra de outro consumidor diretamente, o que foi proporcionado pelas Redes Sociais. Sendo assim, o Social-SAC é o balcão de atendimento do cliente presente nesse novo ambiente.

Para uma empresa implementar um Social-SAC, deve levar em consideração alguns aspectos importantes para que se tenha proteção jurídica e não um risco para sua reputação. O primeiro ponto a observar é: qual o objetivo que se quer com essa presença da marca em um local como o Facebook ou o Twitter? Há intenção de apenas delimitar o território, ou seja, criar um perfil oficial para evitar que outro se passe pela empresa, de prestar informações e esclarecimentos? Ou de fato a empresa está disposta a se relacionar e até mesmo a tirar dúvidas e ouvir reclamações neste canal? Este último caso, sim, configura então o Social-SAC.

Em seguida, a partir da proposta do canal, deve-se verificar: quem é o público-alvo e qual o hábito de navegação digital dele nas redes sociais? Se o público é jovem, já da geração Y, que costuma estar conectado após as 18 horas, então a empresa terá que se preparar para responder aos comentários também nesse horário. Deve ser criado um SLA (*Service Level Agreement*) que deixe claro qual o tempo de demora na resposta que será praticado, que pode ser categorizado inclusive pelo tipo de situação apresentada. Já há estudos que mostram que as empresas têm se preparado para responder em 30 minutos e até no máximo duas horas uma provocação feita em seu perfil oficial.

Se há a intenção de construir mais relacionamento, a empresa, além do perfil, deve criar uma “fanpage”, ambiente mais adequado para divulgar ações promocionais e de comunicação. Pode ainda ser criado um aplicativo para cadastro de participantes, trazendo essas informações para a empresa. Mas, para tanto, deve haver publicação de uma política de privacidade. A questão do uso dos dados dos consumidores é extremamente delicada e, quanto maior a transparência, mais clara fica a regra no momento da interação com o cliente, e mais protegida estará a empresa.

Determinados, então, objetivo, público-alvo, horário de funcionamento e tempo de resposta, deve-se deixar tudo isso claro com vacinas legais nas interfaces gráficas. Se o Social-SAC não for funcionar 24 horas por dia, é essencial publicar outro canal de contato que o cliente possa ser atendido em situação de urgência, que requeira uma resposta imediata (um número 0800, por exemplo).

Há dois grandes riscos para as empresas nessa nova realidade de redes sociais: a) não estar presente; b) deixar o cliente sem resposta. Já há muitas ações judiciais em que o cliente fez o seu protesto nas redes sociais e o conteúdo serviu para documentar a negligência e falta de atenção da empresa para com ele. O próprio PROCON afirma que as redes sociais já geram mais prejuízo às marcas no sentido de imagem negativa (já que todos ficam sabendo, está publicado no mundo), do que as ações judiciais (que em geral ninguém fica sabendo). Essas duas situações geram um grande prejuízo à Marca Digital. Já há formas até de avaliar o valor da marca nas redes sociais, considerando o volume de conexões da mesma e a qualidade do conteúdo associado (*social digital brand value*).

Segundo Luciano Palma, o consumidor espera da página oficial da empresa nas redes sociais: a) transparência; b) estar apta para solucionar um problema imediatamente, com linguagem adequada, maturidade e consciência na resposta; c) ter cultura e estar a par de como funciona a interatividade das redes sociais, que é uma via de duas mãos, em que a empresa fala e há uma resposta e todos estão vendo.

Por certo, o novo *social consumer* vai preferir e escolher as marcas que já estejam atualizadas e presentes nas redes sociais. Pois ele não vai querer encostar a barriga no balcão, nem telefonar, nem mandar um *e-mail*. As empresas devem levar mais a sério essa mudança de comportamento, que é profunda, e atuar mais profissionalmente nas redes sociais, com um plano estruturado e não um “puxadinho digital”. Isso pode fazer toda a diferença.

O diálogo e a própria presença são elementos que geram maior proteção reputacional. Há necessidade de monitorar o ambiente, em caso de incidente, abordar de forma educada. Às vezes, o envio de uma notificação extrajudicial já solicitando para que o consumidor pare de usar o nome da marca pode piorar o caso.

O próprio jurídico deve agir de forma mais estratégica, mais amistosa, com um tom de comunicação que aproxime e não rivalize as partes. Um *post* simpático pode ser muito mais eficaz que uma ação judicial. Devemos educar o próprio cliente a fazer sua reclamação de forma ética, sem difamar, sem ofender, orientando o mesmo por meio da interface gráfica.

Essa atitude de responsabilidade social na era da transparência digital determina quem vai se tornar uma *pocket brand*, ou seja, uma marca de bolso, que todos querem ter a um toque de distância no seu celular, no seu *tablet*, no seu computador, na própria nuvem, convivendo, consumindo, se relacionando, crescendo e criando um Brasil Digital sustentável.

8.7. Propriedade intelectual e o direito autoral nas novas mídias

No Direito brasileiro, o direito autoral³⁸ está protegido pela Constituição Federal de 1988, bem como por lei específica, com previsão inclusive de crime pelo Código Penal em vigor³⁹. Faz-se necessário destacar que o direito autoral, em princípio, protege o titular do direito de autor. Parece algo simples e óbvio, mas, muitas vezes, este detalhe passa despercebido pelo usuário-consumidor do direito autoral, dos conteúdos em geral, bem como pelos concorrentes.

É importante frisar que o direito autoral tem dois aspectos⁴⁰: um patrimonial⁴¹, que significa a valorização do trabalho de inovação e sua remuneração adequada, e outro moral⁴², que representa a proteção à integridade da obra. Com o avanço da tecnologia, a facilidade de se modificar obras é muito grande; no entanto, também existem *softwares* que permitem a criação de uma chave de proteção da obra original, assim como impressões digitais que identificam uma obra autêntica, ou seja, não alterada.

Além disso, o autor só pode ser pessoa física, já o titular do direito autoral pode ser pessoa física ou jurídica.

Dentro do Direito Digital, um fator determinante para o estudo do direito autoral está atrelado à desmaterialização de seu suporte físico. A obra não é mais distribuída em seu modelo tradicional, como, por exemplo, em livro ou CD, ela é acessada pelo usuário. O entendimento deste novo formato de distribuição é essencial para se criar formas de proteção do direito de autor na era digital e também para compreender o motivo que leva a um comportamento coletivo crescente de “que se está publicado na Internet então é público, então pode pegar”.

O Direito não protege a ideia pura, pois essa proteção se confere em um estágio inicial do pensamento, de forma prematura. Caso houvesse tal proteção, poderia gerar um prejuízo à intenção ou à própria inovação. A ideia é uma

38. Direito autoral no Brasil é protegido pela Lei n. 9.610/98, além de ser também um princípio constitucional explicitado no art. 5º, XXVII e XXVIII, da Constituição Federal, e no Código Penal, no art. 184.

39. Art. 2º da Lei n. 9.610/98.

40. Art. 22. da Lei n. 9.610/98: “Pertencem ao autor os direitos morais e patrimoniais sobre a obra que criou”.

41. Arts. 28 a 45 da Lei n. 9.610/98.

42. Arts. 24, 25 e 26 da Lei n. 9.610/98.

constatação de um fato observado com a visão crítica de um observador. No momento em que se torna implementável, torna-se protegida pelo Direito.

A intangibilidade trazida pela Sociedade Digital impõe um grande desafio para os operadores do Direito, já que provoca a necessidade de se repensar o próprio modelo econômico de exploração da propriedade intelectual⁴³. Isso já vem ocorrendo há bastante tempo, mas com a facilidade de acesso e as tecnologias de reprodução, a situação de infração deixou de ser uma exceção, uma ocorrência pontual, para se tornar não apenas comum, mas também “socialmente aceita”. Já ouvi frases como “mas se não é para copiar por que tem o gravador de CD/DVD”?

Não existindo exemplar material fica difícil identificar quando ocorre o “esgotamento da obra”. E isso repercute diretamente na questão socioeconômica do direito autoral, já que a obra torna-se permanente. Há muitas pessoas que se sentem lesadas se, ao comprarem um *software* via Internet, instalarem tal *software* em seu computador, posteriormente sofrerem um problema com vírus que exija reformatar o equipamento, e com isso terem que comprar novamente o *software*, já que o pagamento foi para baixar o programa (*download*), e este não gera um direito por prazo indeterminado para consumir a obra. Como analogia, imagine que após comprar um livro a pessoa o perde, tem o mesmo furtado, queimado, e aí retorna na livraria com o recibo pleiteando um novo exemplar. Logo, o que está sendo comercializado de fato é um direito preso em um suporte, quando não há mais suporte surgem diversas situações de lacuna jurídica ou que o direito ainda não consegue endereçar uma resposta adequada.

Muitos contratos com editoras já trazem previsão de comercialização via Internet, por quantidade de acessos, além do que já preveem normalmente sobre tiragem, de modo a já estarem de acordo com os sistemas de distribuição tradicionais — Livro, e os sistemas de distribuição virtuais — acessos, *clicks* e *downloads*. Esta desmaterialização da obra termina por diminuir os limites temporais entre reprodução, difusão e circulação, que passam a ocorrer quase simultaneamente.

43. O art. 2º da Convenção de Estocolmo de 1967, que estabeleceu a OMPI (Organização Mundial da Propriedade Intelectual), alterada em 1979, define que “a expressão Propriedade Intelectual abrange os direitos relativos às invenções em todos os campos da atividade humana, às descobertas científicas, aos desenhos e modelos industriais, às marcas industriais, de comércio e de serviço, aos nomes e denominações comerciais, à proteção contra a concorrência desleal, às obras literárias, artísticas e científicas, às interpretações dos artistas intérpretes, às execuções dos artistas executantes, aos fonogramas e às emissões de radiodifusão, bem como os demais direitos relativos à atividade intelectual no campo industrial, científico, literário e artístico”.

A complexidade autoral abrange não apenas obras escritas, mas, por analogia, a correspondência eletrônica, os programas de computador⁴⁴, os artigos e conteúdos transferidos nos servidores, os bancos de dados⁴⁵, as imagens criadas como as produzidas em computador ou *scanner*, cujo critério de identificação e tutela do direito se dá por análise de sua originalidade.

Destaque-se que o direito autoral surgiu justamente para proteger a inovação e ao mesmo tempo equilibrar a vontade do acesso público e coletivo da obra (que ocorre quando cai em domínio público) e a remuneração de seu criador para retornar o investimento feito em sua criação.

Não proteger o direito autoral na Sociedade do Conhecimento é o mesmo que estimular a paralisia de pensamento. Por que criar algo se copiar é mais fácil afinal?

Quando a discussão vai para a produção de conteúdos de entretenimento, verifica-se que o problema é muito mais de quebra de expectativas na relação de consumo (não enxergar o custo x benefício do original x pirata), devido ao fato de que, até então, a indústria não precisava se preocupar com o que o cliente queria, já que monopolizava o meio de acesso às obras produzidas. Neste sentido, de certo modo, temos de concordar que a Internet democratizou o acesso aos conteúdos, revelando, inclusive, novos talentos, que pelo modelo tradicional da indústria jamais teriam tido a mesma oportunidade de se tornarem conhecidos e famosos.

Tudo isso que expusemos é para dizer que a Lei ainda precisa de algumas melhorias, especialmente no tocante à questão de “uso justo” (do inglês *fair use*), do “direito a uma cópia de manuseio”, entre outros. Na verdade, a Lei já diz que cabe ao autor determinar, logo, de certo modo, os autores podem criar lei em seu caso concreto, decidindo o que querem ceder ou não de seu direito.

Não se pode permitir a formação de uma geração de plagiadores⁴⁶, de copiadores, de pessoas que dizem “achei no Google”. O Direito deve proteger o autor para proteger a própria evolução da Sociedade.

No âmbito da Internet, quer seja o acesso via computador, TV, telefone, *palm*, *pager* ou outra via convergente, esta questão Autoral toma maior relevân-

44. A proteção ao programa de computador (*software*) é dada pela Lei n. 9.609/98.

45. Art. 7º, XIII, da Lei n. 9.610/98. Neste sentido se manifesta também a Justiça britânica que decidiu pela ilegalidade da utilização de base de dados alheia, ainda que parcialmente, na apelação movida pelo Conselho Britânico de Corrida de Cavalos contra a Organização William Hill, um provedor de apostas à distância.

46. No Brasil, na época colonial, já havia a tipificação do crime de plágio no Código Criminal do Império, de 1830.

cia, pois trata-se de um meio de fácil divulgação e transmissão de informações, fácil acessibilidade e ausência de territorialidade, o que permite que se façam cópias do material que circula na rede com muito mais rapidez, propiciando um maior desrespeito aos direitos do criador e desafiando os métodos atuais de proteção intelectual. Há tecnologias protetivas, mas é preciso também investir em educação e gerar a punição dos infratores.

Assim como em uma guerra, é mais fácil quando se sabe quem é o adversário. No caso dos titulares dos direitos autorais, cada pessoa é um potencial infrator, em uma medida pequena, quando analisada em um contexto meramente de comportamento individual, mas com um poder devastador quando verificado em cenário mais macro, com a soma de todos os usuários-infratores.

É importante destacar que o acesso a dados lançados na rede não os torna de domínio público, não outorgando ao usuário o direito de dispor dos mesmos da forma que lhe aprouver. Estando ou não na forma digital⁴⁷, o Direito deve proteger a criação humana, o direito imaterial. Mas a falta de controle e coerção permite que aconteça na *Web* o que já ocorre com relação a cópia de livros, só que em uma dimensão muito maior. Estas violações constantes prejudicam não só o autor como, principalmente, o próprio Direito que fica desmoralizado perante os infratores e toda a Sociedade. Toda conduta delituosa com alto grau de assiduidade leva ao descrédito da norma jurídica a que se refere.

Estas questões de direito de autor são tão relevantes que têm a adesão de vários países, sendo a Convenção para a Proteção de Obras Literárias e Artísticas de 1886, conhecida como Convenção de Berna, e a Convenção Universal sobre Direitos do Autor, de 1952, conhecida como Convenção de Genebra, as mais importantes. Frise-se que, por serem convenções internacionais, estamos menos sujeitos ao problema da escolha da lei aplicável à matéria, mas devemos conseguir definir em qual território ocorreu a ofensa ao direito de autor para poder lhe dar a jurisdição competente.

Não podemos deixar de considerar e avaliar a revolução causada pelo Napster⁴⁸, sistema que permite a troca de músicas em escala mundial com

47. Art. 7º, *caput*, da Lei n. 9.610/98: "São obras intelectuais protegidas as criações do espírito, expressas por qualquer meio ou fixadas em qualquer suporte, tangível ou intangível, conhecido ou que se invente no futuro,..."

48. Vale citar aqui que a 9ª Corte de Apelação de San Francisco em relação ao litígio entre a Associação Americana da Indústria Fonográfica (RIAA) e a empresa Napster Inc. determinou que a última excluiu de seu sistema as faixas, sobre as quais a Associação Americana da Indústria Fonográfica detém direitos sobre os fonogramas correlatos.

qualidade perfeita de áudio, que colocou em polvorosa as gigantes do mundo das gravadoras e trouxe a questão dos direitos autorais para o centro da discussão na Internet.

Historicamente, sabemos que o Direito Autoral passou a ser mais discutido a partir do surgimento das tecnologias de replicação de conteúdos. Antes da invenção da imprensa, não existiam grandes discussões sobre a matéria, pois se tratava de casos isolados. A valorização do autor trazida pelos movimentos intelectuais da era moderna e a expansão dos meios de reprodução das obras colocaram a questão no centro dos debates internacionais.

Sabemos que a Internet eleva as possibilidades de replicação de conteúdo à máxima potência. O Direito Autoral brasileiro considera qualquer cópia com fins lucrativos, sem a autorização expressa do autor⁴⁹, como uma violação dos direitos autorais⁵⁰. A questão fundamental então para a avaliação da matéria é: a violação do direito autoral tem de sempre vir em conjunto com a geração de uma receita para configurar lesão a direito?⁵¹ E se todos fizerem sua própria cópia? E se o dono da máquina de copiar que cobra para fazer a cópia, que tem um ganho financeiro, este ganho poderia ser considerado então como geração de lucro em cima da cópia dos direitos autorais de terceiro? Estaria ele infringindo o direito autoral mesmo que a pessoa que tira a cópia, que contratou seus serviços de copiadora, não venha a comercializar o livro depois de copiado?

Tecnologias como o Napster e similares disponibilizam uma grande quantidade de conteúdo de forma absolutamente gratuita. Dentre os *softwares* mais conhecidos estão, além do Napster, o Gnutella e o Freenet. A mecânica utilizada por eles permite a busca e a cópia de informações de arquivos armazenados nos computadores de usuários que estejam, naquele momento, conectados a determinado *site*. No entanto, a problemática jurídica não reside no compartilhamento de arquivos via Internet, mas sim no fato de tais arquivos

49. Art. 29 da Lei n. 9.610/98: "Depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades, tais como:

I — a reprodução parcial ou integral;

(...)

X — quaisquer outras modalidades de utilização existentes ou que venham a ser inventadas".

50. "Direito Autoral. Reprodução Fraudulenta. Solidariedade do Vendedor — A solidariedade do que vende ou expõe à venda obra reproduzida com fraude não prescinde da comprovação de culpa" (3ª Turma, STJ, Rel. Min. Dias Trindade — RE 6.087-MG).

51. Art. 46, II, da Lei n. 9.610/98: "Não constitui ofensa aos direitos autorais:

(...)

II — a reprodução, em um só exemplar de pequenos trechos, para uso privado do copista, desde que feita por este, sem intuito de lucro".

serem disponibilizados, na maioria das vezes, de forma gratuita e sem autorização dos autores das obras ou pagamento dos direitos. Pela lei atual, basta a reprodução não autorizada de uma obra para caracterizar violação do direito de autor. Então, respondemos às questões acima levantadas, mas, mesmo assim, a avaliação é dada caso a caso devido à complexidade desta matéria.

A questão que se coloca é até que ponto essa prática como a do Napster pode ser considerada violação dos direitos autorais? E o autor que tem seu próprio *Website*, de certo modo permitindo a disponibilização do conteúdo intelectual na *Web*, que tem por característica ser uma rede de compartilhamento de dados, estaria concedendo uma autorização tácita ou não?

Ao mesmo tempo que a indústria de conteúdo precisa de proteção, ela precisa também de visibilidade — e por isso muitos artistas independentes defendem o Napster, pois este trouxe uma visibilidade a suas criações que o sistema de grande indústria jamais permitiria, principalmente os artistas iniciantes que não têm muitas oportunidades de mostrar seu trabalho. Então, neste sentido, esta tecnologia passa a ser uma ferramenta de Democracia e Liberdade de Expressão, princípios estes protegidos pela Constituição Federal de 1988.

Para aumentar nosso conhecimento há pesquisas que mostram que os consumidores tendem a adquirir determinado produto mais facilmente após tê-lo experimentado. É por isso que se tem uma indústria de sachês, que são colocados em revistas, jornais, PDVs, supermercados, entre outros. A tecnologia do Napster foi apenas uma entre muitas existentes ou a serem criadas para facilitar o acesso do consumidor ao produto e permitir sua experimentação, seu uso. Veremos mais adiante que é possível não cometer violação a direito autoral se for caso de “uso justo”.

Esses avanços tecnológicos são enxergados como alavancadores de negócios pela própria indústria. No entanto, a diferença é que, no mundo virtual, ao contrário do mundo real, como vimos, os bens têm caráter inesgotável. A velocidade de replicação de conteúdos associada ao fato de muitos produtos virtuais não se esgotarem nem se exaurirem, faz com que o que poderia ser bom torne-se ruim, prejudicando e até afastando o momento tão desejado da compra do produto. Então, poderia haver um limite quantitativo ou temporal? Pode ser uma alternativa.

Além disso, é importante enxergar essa questão também sob a ótica do consumidor. A tecnologia multimídia associada a um canal de venda direto, chamado Internet, permite que os consumidores descubram por si mesmos os seus músicos favoritos — e que estes músicos podem não ser necessariamente

aqueles que a empresa quer vender em determinada temporada. O poder está na mão deste consumidor informado, que quer adquirir um produto mais personalizado. A visibilidade da Internet quebra o protecionismo que o mercado criou em torno de si. A lição dada na indústria fonográfica foi do consumidor, muito mais que da própria tecnologia.

Com a alta circulação de conteúdos, produtos e serviços na Internet têm sua legalidade nem sempre atendida, pela falta de autorização ou licença dos seus proprietários ou detentores dos direitos de propriedade intelectual para divulgação, compartilhamento e outras formas de exposição. Por isso crescem as iniciativas de combate à pirataria e outras práticas ilícitas na Internet. Um exemplo é o projeto de lei norte-americano (SOPA — *Stop Online Piracy Act*), que visa combater atividades desde a distribuição, publicação ou transmissão não autorizada de conteúdo protegido (*copyrighted*), passando pelo comércio de serviços ou produtos perigosos aos americanos, e chegando até a ameaças para a economia americana vindas de fora dos Estados Unidos da América. Esse projeto de lei inova quando prevê a responsabilização não somente dos *sites* que oferecem os serviços de hospedagem de conteúdo, mas também dos serviços de busca na Internet, provedores de pagamento e *sites* de publicidade que estiverem envolvidos na cadeia de *sites* estrangeiros infratores. A estratégia é tentar fechar toda a cadeia que alimenta e sustenta os *sites* considerados infratores que, dentre outras condutas, ilegais, hospedam, publicam ou permitem a distribuição do conteúdo descrito acima.

Este projeto quer ir além das fronteiras físicas, considerando como infratores os *sites* que não são dos Estados Unidos da América e que se enquadram nas condições vedadas, cuja responsabilidade de bloqueio de acesso aos mesmos recaem sobre os provedores de serviços, busca na Internet, provedores de pagamento e *sites* de publicidade.

O principal desafio de qualquer lei de combate à pirataria é como garantir a sua eficácia. Isso só ocorre se envolver os provedores de acesso e provedores de páginas que permitem publicação de conteúdo por terceiros e empresas de hospedagem de *sites*. Caso contrário, uma lei ou uma ordem judicial não conseguirão atingir seu objetivo.

Vale lembrar que o Direito é reflexo do modelo socioeconômico estabelecido. Logo, antes de criar uma legislação melhor, é importante rever o modelo de negócios. A princípio, aquele que lucra com conteúdo de terceiro é que deve remunerá-lo. Além disso, deve haver garantia ao acesso à informação pelos internautas e conscientizá-los da necessidade de cumprir com ética e legalidade o uso do serviço oferecido.

Qualquer lei da era digital sempre será envolta em polêmicas. Por isso insistimos em deixar claras as regras do jogo. As empresas da era da Internet que criam novos serviços devem prever os riscos e não podem lucrar com práticas ilícitas. O que é inquestionável é que o criador, inventor, precisa ser protegido, sob pena de sabotarmos a própria Sociedade do Conhecimento.

A solução de Direito Digital deve atender não apenas conteúdos e formatos de negócio conhecidos, como é o caso da música. Deve atender novos produtos como o *e-book* e o *video-on-demand*, onde os autores necessitam de proteção jurídica não apenas tradicional, em tiragem e publicações, mas também a previsão contratual da quantidade de *downloads* e *clicks* autorizados, como já mencionamos. O Direito e a proteção jurídica são sempre os mesmos, o que muda na verdade são os meios e a tecnologia de acesso e reprodução que devem estar sempre citados e exemplificados nos contratos de direito autoral, para não dar margem a dúvidas.

Sendo assim, podemos dizer que o próprio mercado vai se autorregular no sentido de que obras originais valem mais do que obras modificadas, e este critério de veracidade e originalidade é que vai conduzir as relações comerciais e indiretamente proteger o aspecto moral do direito de autor. A busca pela autenticidade da obra é que vai ser a maior proteção contra a lesão ao direito moral do autor. Até lá, caberá à justiça decidir os casos concretos⁵².

52. Casos na Justiça Brasileira:

— Processo movido por Archimedes Messina contra SBT — TV4, alegando ser compositor da música “Sílvia Santos Vem Ai” e que jamais teria sido remunerado por esta. O TJSP acolheu o pleito autoral, condenando o SBT ao pagamento de 500 salários mínimos e multa diária (TJSP — Processo n. 241.691-4/5).

— Em 2005 o SBT passou a exibir o *reality show* “O Grande Perdedor”.

Imediatamente José Braz Lima entrou com ação de indenização, alegando que em 2002 ele havia idealizado tal programa, registrado sua ideia em cartório e enviado carta proposta para o SBT. De acordo com ele, o SBT teria se aproveitado indevidamente de sua criação. O SBT contestou alegando que havia adquirido o formato do programa da empresa norte-americana Reveille LLC e que não há proteção autoral no Brasil para as ideias genéricas. A justiça decidiu que “*não obstante a identidade da ideia central dos programas, isso não traz consequências positivas para os autores, uma vez que as ideias não são objeto de proteção como direitos autorais*”. “*O Direito Autoral não protege ideias simples, comuns, mas sim a sua exteriorização concreta original, artística e perceptível aos sentidos do homem*” (Sentença, Processo n. 1560/05 da Comarca de Osasco).

— Em 1989, Hilton Accioli compôs o jingle “Lula Lá”. Em 2002, o PSDB veiculou, durante a Campanha Presidencial de José Serra, a mesma música, mas mudando a letra para “Serra Lá”. O Autor da Obra ajuizou ação alegando que lhe era devida indenização, uma vez que não havia autorizado tal uso da música. O PSDB contestou afirmando que se tratava de simples gozação, o que era comum e aceito no mercado publicitário. A justiça decidiu que “a

Finalmente, em termos de competência para dirimir conflitos, novamente, devemos ter em mente que o Direito Digital é um direito comunitário, multicultural e dinâmico; portanto, a melhor solução é via mediação e arbitragem, podendo ser estabelecido a que legislação quer-se ter referência, se a do lugar de origem do fato danoso, se do lugar do resultado do fato danoso, se do lugar da origem da obra, ou se pelo conjunto normativo que possibilite chegar a um denominador comum, um acordo.

8.8. Domínios

O estudo do tema de domínios é novo no Direito, tendo em vista que o nascimento deste conceito está totalmente atrelado ao surgimento da própria Internet. Diferentemente do registro de marca, o registro de domínio não está dividido em categorias por ramos de atividades. O que torna a sua disputa ainda mais acirrada⁵³.

Devido à relevância atual da presença na Internet para muitas empresas, o domínio passou a ser muito mais que o representante virtual do ponto comercial. O que se quer dizer é que eles determinam a visibilidade da empresa e a capacidade de ela ser localizada; quando não imprimem também valor.

Apesar de o domínio se referir ao endereço virtual da empresa, este tem características distintas da concepção tradicional aplicada ao mundo físico, já que normalmente o endereço não necessariamente agrega valor a determinada empresa, da forma como o domínio o faz no mundo virtual. Isso porque uma empresa será mais facilmente localizada no emaranhado da rede quanto mais

situação criada não tinha nada de humorístico e, sim, muito pelo contrário, fazer a população desacreditar no candidato adversário, no caso o Lula. Em que pese toda a imaginação e criatividade do réu em utilizar, dessa forma, trechos da obra do autor, essa estratégia foi infeliz na medida em que não houve autorização por parte do autor, criador e titular dos direitos da obra. A própria testemunha Rui Sergio declarou que não sabia dizer o porquê de não terem consultado o autor” (Sentença, Processo n. 080.286/03 da Comarca de São Paulo).

— Processo movido por Luiz Eduardo Régner Rodrigues contra Newcomm Bates Comunicação Integrada Ltda. e Cervejarias Kaiser Brasil Ltda., argumentando que havia criado a campanha e *slogan* usados pelas rés. O STJ decidiu que era devida indenização, mesmo que a obra do autor não tivesse sido divulgada (STJ, REsp 655.035 — Rel. Min. Humberto Gomes de Barros).

53. No Brasil o registro de nomes de domínio é de competência do NIC.br, de acordo com as Resoluções n. 1 e 2, de 2005, e n. 1, de 2006, do Comitê Gestor da Internet no Brasil (CGI.br), sendo estas últimas revogadas pela Resolução n. 8, de 2008.

próximo o nome de seu domínio for de sua marca⁵⁴. Com o crescimento vertiginoso da Internet, isso se torna quase que um requisito para “ser encontrado”.

Para o Direito Digital, o domínio na Internet não é apenas um endereço eletrônico, mas sim a união entre localização (endereço) e valor de marca (capacidade de ser lembrado — *awareness*). Deter o nome de uma empresa na rede é deter-lhe o valor; é deter-lhe a capacidade de ser alcançada por seu público-alvo, o que pode representar um sério problema, especialmente no caso de marcas conhecidas do público em geral⁵⁵.

Por ser uma “nova terra”, o espaço virtual atrai também aproveitadores, oportunistas, verdadeiros “grileiros” virtuais, indivíduos que registram como domínios os nomes de marcas conhecidas, com a finalidade de negociar estes domínios com os legítimos titulares das marcas.

Há, ainda, a prática do *cybersquatting*⁵⁶, que consiste em registrar domínio igual ou semelhante à marca famosa visando ganhar dinheiro com isso, e a

54. No Brasil o registro de marcas e patentes é competência do INPI, de acordo com a Lei de Propriedade Industrial (Lei n. 9.279/96).

55. Uma das empresas que mais propôs ação para proteger o nome de domínio, foi a América Online (AOL), que litigou contra a empresa curitibana América On Line Telecomunicações Ltda. pelo domínio www.aol.com.br e só conseguiu atingir seus objetivos por meio de um acordo entre as partes que também ganhou as páginas dos jornais (*Jornal Valor*, p. E1, 25-9-2001) ao obter da Justiça Federal do Rio de Janeiro todos os efeitos pretendidos numa ação que foi indeferida por impossibilidade jurídica do pedido. A empresa pedia para que fossem registrados e declarados os nomes AOL e América Online como marcas notórias (o que não é mais possível desde 1997 com a Lei de Propriedade Industrial). Apesar disso, a Juíza Daniela Milanez expediu uma ordem judicial que obrigava o INPI a incluir a AOL na lista de marcas notórias da Fapesp, responsável por esse feito na época.

56. Neste caso podemos citar o seguinte caso:

Tribunal de Justiça de São Paulo

Apelação Cível n. 497.069.4/0-00

Juízo de origem: 19ª Vara Cível Central da Capital.

Processo n: 05.018676-7

Aptes.: DM Indústria Farmacêutica Ltda. e outra.

Apdos.: Avanço Informática e outro.

VOTO n. 2328

AÇÃO ORDINÁRIA — Domínio de marca virtual e indenização — ação julgada parcialmente procedente, determinando o cancelamento do registro do nome do domínio e a abstenção do uso da palavra “avanço” ou na forma “avanço”, afastando o pedido de indenização. Recurso da autora pleiteando a condenação em verbas indenizatórias. Recurso da ré sustentando a ausência de demonstração da notoriedade ou alto renome da marca. Comprovação do uso indevido de marca de renome, que atrai seus consumidores — o produto ou serviço representado pela marca é protegido pela legislação, visando coibir a concorrência desleal — ausência de considerações acerca dos danos — existência de prejuízo não reconhecida — afastando o direito a indenização por perdas e danos sofridos.

Recursos desprovidos.

Trata-se de recurso de apelação interposto contra a r. sentença (fls. 329/332), declarada a fl. 364, cujo relatório é adotado, que julgou parcialmente procedente o pedido para determinar o cancelamento do registro do nome de domínio “avanco.com.br” levado a efeito pela ré, junto à Fapesp, e a abstenção por parte da requerida de o utilizar, assim como, de qualquer outra forma, a palavra isolada “avanço” ou “avanço”, sem que permita ao consumidor claramente distinguir da marca “avanço”, de titularidade da autora. Em síntese, após considerações sobre a decisão, a DM Indústria Farmacêutica Ltda e Papyrus LLC, por considerar que a contrafação gera direito a indenização, que pode ser apurada em liquidação, pedem a condenação da ré-recorrente no pagamento dos danos ocasionados (fls. 334/340). A Avanço Informática Ltda., por sua vez, voltou a sustentar que a autora não apresentou nenhum título ou documento capaz de demonstrar a notoriedade ou o alto renome da marca.

Considera questionável se falar em alto renome em torno de uma marca que não seja singular, ou seja, que conviva com diversas outras, pelo que pede a reforma do *decisum* (fls. 365/375). Processados os recursos, foram apresentadas contrarrazões (fls. 380/387 e 389/394).

É o sucinto relatório.

Ingressou a apelante DM Indústria Farmacêutica Ltda. e Papyrus LLC com a presente ação de indenização, pleiteando o cancelamento do registro de domínio da Internet “avanco.com.br”, uma vez que a marca “avanço” lhes pertence e é de seu uso exclusivo. Contrariamente, a recorrente Avanço Informática Ltda. sustentou que seu objeto social se liga ao desenvolvimento de *softwares* e que a marca “avanço”, por não gozar de notoriedade, não é suscetível de obter proteção para todas as classes do classificador NICE, como se fosse de alto renome.

Em sua decisão, a MMA. Juíza sentenciante considerou que “O site, assim como formulado, remete de plano e, incondicionalmente, à conhecida marca ‘avanço’, o que inexoravelmente traduz em uso indevido, porquanto atrai, por meio de marca de renome da autora, consumidores desta, que buscam ou visualizam a referência site” (fls. 330/331).

Marcelo Junqueira Inglês de Souza, tecendo considerações sobre “Marca”, dentre outras coisas, ensina que “... sob o enfoque jurídico, o direito marcário protege o produto ou serviço que é representado pela marca... O direito visa coibir a concorrência desleal, protegendo o esforço, o investimento, o trabalho, o sucesso do empreendedor; impedindo que o mesmo tenha concorrente desleais...” Ainda, que “a legislação marcária também procura resguardar o consumidor, pois a função principal da marca é facilitar a ele a identificação de um produto, bem ou serviço, de uma empresa, diferenciando-os de outros idênticos ou semelhantes... qualquer tentativa de utilização ilegal da mesma prejudicará não só o detentor da marca; também induzirá o comprador a erro” (Eliane Y. Abrão — Propriedade imaterial — Senac — 2006 — p. 353/354).

Frente a esses conceitos, não há como acolher a pretensão da recorrente-ré. Sendo marca renomada — a isso não há como negar — a autora logrou através do seu trabalho criar uma interação entre a marca e o produto, de sorte que o consumidor, instintivamente, logo associa a marca ao produto. Assim, não importa que a recorrida apelada atue em ramo distinto (*software*). Ao tentar localizar a marca “avanço” ou “avanço”, através da Internet, o consumidor será direcionado para o site diverso do procurado, o que caracteriza uso indevido de nome, pelo que se mostra correta a decisão, pois evidente a usurpação.

Quanto ao pleito indenizatório, igualmente, nenhum reparo merece a decisão, já que a pretendente deveria, ao menos, tecer considerações a respeito dos danos conhecidos e não apenas fazer pedido genérico a respeito (fl.18).

Como já decidido pelo E. Superior Tribunal de Justiça, “Inadmissível a condenação em perdas e danos, pela confusão provocada junto ao consumidor por marcas semelhantes, se não reconhecida a existência de prejuízo sofrido pela autora” (REsp 613.376/SP — Min. Castro Filho — Terceira Turma — j. 19-9-2006 — DJ de 23-10-2006 — p. 298).

outra modalidade conhecida por *typosquatting*, que ocorre quando uma empresa registra domínio que remete à marca famosa com pequenos erros de digitação, como, por exemplo, netsape.com. Ambas são ilegais por serem consideradas práticas extorsivas.

O problema poderá multiplicar-se com o aumento das opções de TLDs (*Top Level Domains*, as terminações de endereço eletrônico aceitas como padrão na rede), votada favoravelmente pelo ICANN (*Internet Corporation for Assigned Names and Number*, o órgão responsável) em junho de 2008. São utilizadas as terminações “.gov” (para os órgãos governamentais), .edu (para instituições de ensino), “.int” (para determinadas instituições), “.com, .net e .org” (para os demais). Essas terminações, porém, estão em vias de ser ampliadas⁵⁷, passando-se a aceitar outras, como ocorreu nos casos do “.biz, .bank, .shop, .travel, .news, .tv” etc.

Para alguns, tais terminações deveriam ser livres — o que tem gerado situações inusitadas: os dirigentes de um país como Tuvalu (uma ilhota do Pacífico Sul que tira seu sustento da venda de cocos e selos para colecionadores e detém a terminação “.tv”, obviamente visada por empresas de comunicação de todo o planeta) vendeu esta terminação para a companhia norte-americana *VeriSign*, o que efetivamente dobrou seu PIB anual⁵⁸. Se ocorrer o caso extremo, com a liberação geral das terminações, provavelmente os grileiros voltarão a atacar com força total.

Tradicionalmente, em termos jurídicos e de legislação em vigor, a prioridade de registro é dada pela sua ordem, ou seja, o critério normal é a propriedade para aquele que solicita determinado registro em primeiro lugar, critério

À vista do exposto, pelo meu voto, nego provimento a ambos os recursos, mantidas as verbas da sucumbência.

PAULO ALCIDES

Relator

57. O aumento das terminações de domínio são votados pela International Corporation of Assigned Names and Numbers (ICANN). A ICANN é uma corporação internacional sem fins lucrativos responsável pela alocação do espaço de endereços de Protocolos da Internet (IP), pela atribuição de identificadores de protocolo, pela administração do sistema de nomes de domínio de primeiro nível genéricos (gTLDs) e com códigos de países (ccTLDs) e pelas funções de gerenciamento do sistema de servidores-raiz. Como parceria público-privada, a ICANN se dedica a preservar a estabilidade operacional da Internet, promover a concorrência; obter a ampla representação das comunidades globais da Internet e desenvolver políticas adequadas à sua missão por intermédio de processos “de baixo para cima” e baseados em consenso. A ICANN apoia a Declaração de Túnis adotada durante a segunda fase da Cúpula Mundial sobre a Sociedade da Informação (WSIS) em relação à atual coordenação técnica da Internet. Site: <www.icann.org>.

58. Fonte: <<http://www1.folha.uol.com.br/folha/reuters/ult112u10352.shtml>>.

conhecido como *first to file*⁵⁹. Mas o mau uso desses registros tem tido como solução de Direito Digital a concessão da propriedade do domínio prioritariamente ao detentor da marca no mundo real. Para solucionar possíveis conflitos em relação a determinado domínio na Internet, o requerente deve provar a disponibilidade do registro da marca no mundo real ou a sua propriedade relacionada ao serviço que explora, para então justificar sua utilização e registro no mundo virtual.

Assim, por exemplo, no caso de domínios cujos TLD estejam sujeitos à reclamação no Centro de Arbitragem e Mediação da OMPI, uma das primeiras instituições autorizadas pelo ICANN para fazer disputas relativas a nomes de domínios, esta pode ser feita mediante prova de três itens: que o nome de domínio é igual ou similar à marca registrada; que o reclamado não tem direitos legítimos sobre o nome de domínio; e que o uso do nome de domínio pelo reclamado é de má-fé. Após juntadas ao processo todas as provas possíveis, é eleito um árbitro para analisar e julgar o caso, sendo aberto o prazo para contestação. Após o julgamento, a decisão é remetida às partes e ao órgão que efetuou o registro do domínio, a fim de que este cumpra a decisão.

Uma solução de planejamento estratégico que independe da existência de legislação específica de registros na rede e pode ser adotada pelas próprias empresas é a seguinte: efetuar o registro de domínios com várias combinações possíveis envolvendo os nomes de sua marca. É cada vez mais comum nas empresas a prática de registrar domínios que contenham sua marca de forma depreciativa, para evitar seu uso por terceiros. Se houver o aumento das opções de TLDs existentes, provavelmente haverá uma corrida das grandes empresas para registrar domínios com todas as terminações possíveis. A única questão é quanto ao custo de ter de proceder a todos esses registros, o que torna esta solução um tanto onerosa, principalmente para micro e pequenas empresas.

Muitas vezes, uma atitude de bom senso no intuito de fazer uma rápida análise das possibilidades e implicações acerca do registro de determinado domínio poderia prevenir uma infinidade de litígios, às vezes de difícil solução, nos quais nem sempre o verdadeiro direito é alcançado.

Os nomes de domínio são constituídos por uma sequência de letras e dígitos que identificam o “endereço” de um computador na Internet, correspondendo as referidas letras e dígitos a uma sequência numérica única, permitindo que o referido endereço seja localizado na rede.

59. Art. 1º, *caput*, da Resolução n. 002/2005 (revogada pela Resolução n. 8, de 2008) do Comitê Gestor da Internet (CGI.br).

A utilização do nome de domínio no lugar de números se justifica devido à facilidade que a maioria dos usuários tem em memorizar nomes em vez de séries numerais. Sua atribuição foi um dos primeiros problemas que surgiram na rede em razão da ausência de autoridades imbuídas de poder para supervisionar a Internet como um todo, e em decorrência disso houve a necessidade de serem criados, em cada país, organismos controladores e incumbidos de registrar os endereços ou URL. Compete a estas instituições limitar e não permitir que dois endereços iguais possam ser distribuídos a diferentes usuários, a exemplo do direito de marcas.

Para que a implantação do sistema de distribuição de nomes de domínio ficasse organizada de modo centralizado, foi dada a uma entidade a atribuição para o ato, com o objetivo de evitar a duplicidade de nomes e o próprio controle dos registros. No Brasil a entidade encarregada dos registros atualmente chama-se NIC.br (Núcleo de Informação e Coordenação do Ponto BR).

Por todo o exposto, tem havido uma corrida para obtenção de registros, que se evidencia pelos dados fornecidos no *site* do NIC.br, indicando mais de 1,3 milhão de registros de nomes de domínio por dia no País⁶⁰.

Devidamente exposto, portanto, em que exatamente consiste o nome de domínio e o campo de atuação em que ele se insere, bem como as suas características — e, ainda, a importância e atualidade da questão no Brasil —, essencial se faz, sem dúvida, em face das peculiaridades da matéria, explicitar alguns aspectos jurídicos envolvidos.

Entre as resoluções pelo “CGI.br”, a Resolução n. 002/2005, revogada pela Resolução n. 008/2008, regulamenta o registro de nomes de domínio no País. Conforme o art. 1º da mencionada resolução, o registro de um nome de domínio disponível será concedido ao primeiro requerente que satisfizer, por ocasião do requerimento, as exigências para o registro, conforme as condições descritas nessa resolução e em seu anexo. Assim, em tese, a primeira pessoa jurídica que requerer o registro de nome de domínio disponível, estando em conformidade com as regras formais para o seu registro, poderá obtê-lo, independentemente de qualquer exame de mérito pelo CGI.br ou pelo NIC.br.

Isso se dá em decorrência do teor do disposto no § 10 do mesmo art. 1º, que estabelece constituir obrigação e responsabilidade exclusiva do requerente do nome de domínio a escolha adequada deste, sendo que terá de se declarar ciente de que não poderá ser escolhido nome que desrespeite a legislação em

vigor, que induza terceiros a erro, que viole direitos de terceiros, que represente conceitos predefinidos na rede Internet, que represente palavras de baixo calão ou abusivas, que simbolize siglas de Estados, Ministérios, dentre outras vedações.

Diante de tais dispositivos legais, conclui-se que, muito embora não exista um exame de mérito por parte dos órgãos responsáveis pelo registro dos nomes de domínio do Brasil, estes não podem infringir, entre outros, direitos de terceiros, o que é de responsabilidade exclusiva do requerente. Tal constatação afasta o argumento, por exemplo, de que, se não há direito ao registro de determinado nome de domínio, o NIC.br deveria barrar a pretensão. De fato, existem alguns nomes de domínio aos quais o NIC.br, de ofício, barra o registro, mas tal listagem não é exaustiva ante as inúmeras marcas e direitos de terceiros existentes e que podem, efetivamente, ser violados com o registro de um nome de domínio.

Por falar de domínio, e estar este muitas vezes atrelado a marcas, é essencial tratar também da proteção jurídica delas em nosso Ordenamento.

As marcas são sinais distintivos visualmente perceptíveis, protegidos pela Constituição Federal, em seu art. 5º, XXIX, cuja proteção é regulamentada pela Lei n. 9.279/96. Equivocadas são as alegações de que o registro de um nome de domínio não pode infringir o direito à marca de terceiro, por se entender que são situações absolutamente diversas.

De fato, a marca e o nome de domínio são figuras jurídicas diversas, com proteções, amplitude e regulamentação distintas. Entretanto, a marca é um direito conferido a terceiro pelo Estado, o que se enquadrava na proibição contida no art. 1º, § 1º, da Resolução n. 002/2005 da CGI.br, agora substituída pela Resolução n. 008/2008, que contempla esse tema em seu art. 1º, § 1º.

Assim como nos registros dos nomes comerciais, das marcas, dos direitos autorais etc., há respeito recíproco, quando houver semelhança que puder trazer prejuízos aos titulares e a terceiros, a proteção do nome de domínio deve harmonizar-se com esses institutos e obedecer ao mesmo princípio.

“As marcas de alto renome e as notoriamente reconhecidas não podem ser registradas como nomes de domínios senão pelos próprios titulares das marcas ou por terceiros devidamente autorizados”⁶¹.

60. Fonte: <<http://www.nic.br/imprensa/clipping/2008/midia282.htm>>.

61. CUSTÓDIO FILHO, Ubirajara. Os conflitos entre marcas e nomes de domínio da Internet no direito brasileiro. In: *Internet — o direito na era virtual*. Rio de Janeiro: Forense, 2001. p. 89-90.

Mais adiante acrescenta o mesmo autor: “Os nomes de domínios que contêm marcas registradas perante o INPI somente podem ser admitidos pelo NIC.br se requeridos pelos próprios titulares dessas marcas, salvo se restar descaracterizada a hipótese de concorrência desleal”⁶².

Mesmo as marcas sem renome especial também não podem, em muitos casos, servir para domínio, sob o risco de configurar o crime de concorrência desleal.

Já há diversas decisões judiciais sobre este tema que relaciona a questão do conflito entre domínios e marcas⁶³.

62. Op. cit., p. 91.

63. Ementa n. 245.984

MARCAS E PATENTES — Agravo em ação cominatória — O registro de domínio na Internet não deve desconsiderar os direitos decorrentes do registro de marca junto ao INPI — A tutela antecipada, preenchidos os requisitos do artigo 273 do Código de Processo Civil, foi bem concedida — Agravo Improvido — AgI 202.504-4/8 — 2ª Câ. de Direito Privado — Rel.: Paulo Hungria — j. 26-6-2001 — v.u.

Ementa n. 254.906

PROPRIEDADE INDUSTRIAL — Nome de domínio — Endereço na Internet — Abstinência do uso — Tutela antecipada — Deferimento — Existência de marca com registro no INPI — Proteção estabelecida no artigo 5ª, inciso XXIX, da Constituição da República — Prevalência, ademais, sobre as deliberações do Comitê Gestor da Internet no Brasil — Recurso não provido — J/TJ 248/325.

Tribunal de Justiça do Rio Grande do Sul — Agravo de Instrumento: 599.132.826 — Agravante: Grendene S/A — Agravada: Riegel Imóveis e Construções Ltda. — www.rider.com.br — Concessão de liminar em sede de agravo, para vedar a utilização da marca RIDER, como nome de domínio e endereço eletrônico da Agravada.

7ª Vara Cível de Guarulhos/SP — Proc. 24.12/98 — Autor: Luk do Brasil Embalagens Ltda. — Réu: Pladis Ingeauto Ind., Com. e Imp. Ltda. — www.luk.com.br — Concessão de tutela antecipada para determinar a cessação do uso do domínio, sob *astreinte*, por caracterizar contrafação.

1ª Vara Cível de Patos de Minas/MG — Proc. 19.048 — Autor: Associação Comercial e Industrial de Patos de Minas — ACIPATOS — Réu: Net Shop Informática Ltda. — www.acipatos.com.br — Concessão de liminar para suspender o uso do nome de domínio, formado pelo nome de Autora, e autorizando esta a registrá-lo em seu nome.

7ª Vara de Fazenda Pública de SP — Proc. 143/99 — Autor: TV Globo Ltda. — Réus: ML Editora de Jornais e Revistas Ltda. — www.jornalnacional.com.br e www.globoesporte.com.br — Sentença cancelando os domínios, em vista das marcas registradas da Autora.

Tribunal de Justiça do Paraná — AC 86.382-5 — Apelante: Laboratório de Aprendizagem Meu Cantinho Ltda. — Apelado: Ayrton Senna Promoções e Empreendimentos Ltda. — www.ayrtonsenna.com.br — Acórdão determinando a abstenção de uso e a transferência do nome de domínio, por contrafação e infração ao direito da personalidade.

22ª Vara Federal/SP — Proc. 199.61.00.009988-8 — Autor: Carl Zeiss e Carl Zeiss do Brasil Ltda. — Réus: Quality Technologies Com. Imp. Exp. / Ltda. — www.zeiss.com.br — Tutela antecipada proibindo a utilização do nome e determinando a sua suspensão, em vista de registro de marca no INPI, para os mesmos produtos.

É importante salientar, de outro lado, que a matéria, no âmbito jurisprudencial, além de escassa, é extremamente controversa, apresentando, assim, entendimentos em ambos os sentidos, como a decisão abaixo:

“A marca e nome de domínio se apresentam como espécies de propriedade industrial, bens incorpóreos que compõem o fundo de comércio, por uma singela razão: a expressão ‘ad’, parte integrante do seu nome comercial, também registrada como marca perante o INPI, não preenche qualquer dos requisitos legais exigidos, ou seja, não constitui marca de alto renome ou notoriamente conhecida, hipóteses estas que — qualquer delas configurada — implicariam a procedência da demanda, ‘mesmo havendo registro precedente na FAPESP’ (Acórdão n. 70003677515 — TJRS). Necessidade de marca de alto renome ou notória para a transferência do domínio”.

Outra decisão interessante ocorreu no Tribunal de Justiça do Estado de São Paulo, em processo movido pela Universo Online Ltda. — UOL e Brasil Online Ltda. — BOL contra terceiro que havia registrado domínio semelhante à marca das autoras. De acordo com o acórdão, “observa-se, portanto, que as coautoras estão sofrendo ameaça de violação ao direito de marca, cuja proteção está prevista na Constituição Federal [art. 5ª, XXIX, da CF] e no art. 129, da Lei 9.279/96, bem como de nome empresarial. A corré pretende usar parte de marca alheia, somada a elemento de uso comum, confundindo as pessoas que procuraram endereço eletrônico como forma de conhecimento”⁶⁴.

Já na sentença publicada na decisão do Processo n. 1.306/2000 da 19ª Vara Cível de Curitiba, o magistrado asseverou que o princípio da especificidade já está pacificado pela jurisprudência do STJ, segundo o qual “o direito de exclusividade do uso da marca, decorrente de seu registro no INPI, é limitado à classe para a qual é deferido, não sendo possível a sua irradiação para outras classes de atividades”. No caso dos autos, “não se vislumbra esteja a ré a aproveitar-se da marca que alega a autora haver construído no ramo mercadológico em que atua, tampouco há notícia de confusão entre as empresas litigantes junto ao público consumidor”.

18ª Vara Cível de Belo Horizonte/MG — Proc. 02499129278-0 — Autora: Telemig Celular S/A — Réu: Paulo Roberto Gentil Alves — www.celularcard.com.br — Tutela antecipada determinando abstenção do uso do nome de domínio, em vista de marca registrada da Autora.

20ª Vara Cível de São Paulo/SP — Proc. 00.513789-6 — Autor: Bloomberg LP — Réu: Confecções New Top Ltda. — www.bloomberg.com.br — Tutela antecipada determinando abstenção do uso do nome de domínio, em vista de marca registrada da Autora.

64. TJSP, Ap. 289.554.4/1-00.

Entendemos que, pelo fato de o domínio desempenhar função identificadora dentro da Internet, seu núcleo, sim, poderá estar relacionado à marca de um produto ou serviço, dependendo da natureza da informação alojada no *site*, e, assim, especialmente, receber proteção nos preceitos da Lei de Propriedade Industrial. Esta distinção se faz essencial para entender por que em alguns casos, devido ao uso de palavras comuns, de baixo calão, ou nome tipificado como não registrável, ou até mesmo de marcas que possuem registros em diversas categorias distintas, e, por sua vez, em cada uma, passam a ser de propriedade de uma empresa distinta; também, muitas vezes, na Internet, o domínio que naturalmente seria considerado de determinada empresa está, no entanto, sob a posse de outra, sem que isso avilte qualquer direito ou configure crime de Concorrência Desleal.

Devido, em especial, ao crescimento vertiginoso da Internet, que já possui, de acordo com *sites* de monitoramento da rede mundial⁶⁵, mais de 500 milhões de *websites*, considerados apenas os domínios de hospedagem principal, esses *websites* passaram a ser fundamentais para que empresas e usuários da Internet, potenciais clientes e consumidores de seus produtos e serviços, sejam capazes de localizar entre os bilhões de endereços disponibilizados aqueles que correspondem à sua empresa, geralmente associados à marca pela qual são reconhecidos.

A ICANN é a responsável pela coordenação global do sistema de identificadores exclusivos da Internet, como os nomes de domínio do tipo TLD (*Top-Level Domain*) e gTLD. Atualmente, uma pessoa ou uma empresa interessada em obter o registro de um nome de domínio deve solicitar ao “register” competente na área geográfica na qual tem interesse. Esse órgão — que no Brasil é o NIC.br — checa junto à ICANN (*registry*) a viabilidade do nome. Se estiver disponível, o interessado pode ter seu registro efetivado. Interessante notar que a ICANN é a responsável por tornar o nome de domínio tecnicamente funcional, ou seja, atrelar o nome apresentado ao número de IP (*Internet Protocol*) correspondente. Nos casos em que há conflito, tem sido usado o registro de marca (no Brasil, o responsável é o INPI) para resolver quem tem preferência ou direito sobre o mesmo.

A Internet passou por mais uma transformação no que diz respeito ao universo mais corporativo. Com o novo programa para registro de domínios aprovado pela ICANN, que teve início em janeiro de 2012, muitas empresas se prepararam para um novo cenário de “Marca Digital Global”. Agora se pos-

sível ter um novo grupo de gTLD, em que bastará o nome da marca como domínio “www.marca”, o que permite maior proteção, internacionalização, massificação, bem como evitar situações recorrentes de registro de domínio com o nome da marca por terceiro não autorizado, diminuindo assim riscos legais e reputacionais.

Com o programa da ICANN para novos domínios, os interessados poderão criar e gerenciar um TLD de sua própria escolha, solicitando-o diretamente à ICANN e não mais ao órgão de registro, como o NIC.br. Nesse novo cenário, o detentor de um TLD faz suas próprias regras, ou seja, pode vender *second level names* como desejar — ou mesmo não vender —, hospedar serviços especializados, estipular que tipos de conteúdos poderão estar debaixo de seu TLD, entre outras infinitas possibilidades. A ICANN recomenda que a empresa que optar por isso esteja amparada pelo conhecimento técnico de pessoas e escritórios especializados em nomes de domínio, visto que o investimento é significativo: apenas para dar entrada no pedido de um gTLD próprio, o interessado precisará desembolsar US\$ 185.000,00.

O processo de análise por parte da ICANN será bastante acurado, com vistas, por exemplo, a coibir a atuação de pessoas de má-fé que desejem obter um TLD com um nome de uma marca da qual não possuam propriedade, e deve levar cerca de um ano após a entrada do pedido. O lado positivo do valor mais elevado é que de certo modo evita um pouco a “grilagem digital”, o “registro oportunístico”.

Interessante ressaltar que uma empresa pode se opor contra terceiros que tentem obter um TLD com o nome de sua marca. Por isso, mesmo que haja a decisão de não pleitear um *top level domain* próprio, grandes marcas devem estar atentas à atuação de concorrentes e demais terceiros, acompanhar os procedimentos.

Finalizamos lembrando que, por diversas vezes, os tribunais reconheceram a prioridade no direito de registro de domínio de Internet às empresas que já possuem o registro da expressão como marca, aplicando-se o princípio da anterioridade.

8.9. Proteção de conteúdos, *websites* e outros direitos autorais digitais

No Direito Digital, o conteúdo toma a forma de bem jurídico a ser tutelado. Esta crescente importância do conteúdo está em sintonia com o que para Don Tapscott é a sociedade digital: “*A Sociedade Digital é fruto da união*

65. Dados de junho de 2008 — <<http://www.isc.org/index.pl?/ops/ds/>>.

dos 3Cs — *Computação, Comunicação e Conteúdo*⁶⁶. Um dos grandes desafios não é a discussão do meio, da comunicação em si ou da tecnologia em si. É a questão do conteúdo, ou seja, da produção intelectual cada vez mais necessária para manter o interesse no uso do meio e na própria tecnologia. Esta produção implica, inclusive, a criação de produtos imateriais dispostos no meio e viabilizados pela tecnologia para serem consumidos, como é o caso do MP3, do *e-book* e do próprio mecanismo de *download*.

A necessidade de regular essas questões traz uma grande semelhança com problemas enfrentados pela propriedade intelectual no começo do século e pela questão das patentes até hoje, principalmente na área farmacêutica e de biotecnologia, visto que há sempre interesses macroeconômicos muito maiores do que apenas a determinação de conceitos jurídicos. Novamente, a relação computação, comunicação e conteúdo determina o monopólio do poder e a soberania dos Estados dentro da Era Digital e, diante de um mundo cada vez mais globalizado, os donos destas “pontes” podem vir a ditar as regras, cada vez mais.

No mundo virtual, o conteúdo tornou-se um objeto de negociação, um produto. A todo momento surge um novo *site* ou portal vendendo conteúdo como uma palavra mágica, um diferencial em relação à concorrência (só que a concorrência também vende conteúdo como um diferencial). O conteúdo na Internet não é gerado necessariamente para um comprador, mas torna-se cada vez mais uma mercadoria cuja posse agrega valor ao seu proprietário.

Sob a ótica do Direito Digital, é importante diferenciar conteúdo de informação. Em alguns casos, o conteúdo pode ser entendido como uma informação à qual se dá crédito (daí o movimento de inúmeros portais em contratar jornalistas de renome, cuja função primeira é transformar a informação disponível em conteúdo). A maior problemática do conteúdo é a sua questão autoral, dado o efeito multiplicador que caracteriza a rede e as inúmeras possibilidades comerciais dela, assim como os novos modelos criados dentro do contexto de uma sociedade cada vez mais convergente.

Assim como nas emissoras de radiodifusão, o conteúdo é que motiva a audiência. No mundo da convergência, uma audiência motivada torna-se também um potencial público consumidor. É prática comum, na maioria dos *sites* e portais, unir conteúdo e comercialização de produtos em uma mesma página. O conteúdo ganha então sua função econômica.

Como vimos, a Internet é uma rede de indivíduos. Por isso, os conteúdos de massa raramente funcionam nesse veículo, que privilegia os conteúdos seg-

mentados — e, conseqüentemente, é o conteúdo que se torna o *link* de contato imediato do consumidor com determinado produto inserido em um contexto e um ambiente que motive o impulso de compra, de um público altamente segmentado e direcionado (os *sites* de relacionamento são o exemplo extremo dessa situação: neles encontram-se desde informações para o mercado financeiro, voltadas para um público de empresários, até fotos de garotas em trajes sumários, buscando conquistar o público adolescente). Com tantos valores agregados, mais o fato de estar sendo disponibilizado em um meio altamente replicável, torna-se complexo estabelecer um valor real para o conteúdo na rede.

Sendo assim, há várias categorias de conteúdo, desde os de acesso restrito, ou seja, conteúdos exclusivos, até os de consumo imediato, como as notícias, cujo valor diminui com o passar do tempo e com a quantidade de acessos, além dos conteúdos qualitativos, elaborados para públicos direcionados e que permitem a alavancagem de *page-views* específicas. Caso a opção de conteúdo represente o sucesso comercial e a fidelização, em muitos casos, então a responsabilidade dos advogados que elaboram os contratos de conteúdo é muito grande. Em linhas gerais, os contratos de conteúdo devem prever não apenas o tipo específico de conteúdo a ser produzido ou que está sendo comprado, como seu valor fixo e variável de acordo com seu resultado de impacto de acesso, sua depreciação e o tempo de vigência. Além, é claro, do responsável editorial por ele.

Como sabemos, o efeito de um conteúdo mentiroso ou calunioso⁶⁷ na Internet pode ser muito mais devastador do que em qualquer outro veículo. Mesmo que uma notícia falsa possa ser rapidamente apagada de um *site*, por exemplo, ela já pode ter sido copiada inúmeras vezes e disponibilizada em muitas outras páginas. Assim como é difícil valorar um conteúdo virtual, é igualmente difícil valorar o tamanho do dano causado por um conteúdo quando passa uma informação errada, calúnia, ou manifesto contra determinada empresa. Ou seja, é praticamente impossível mensurar a extensão do dano; não há controle de tiragem e nem se sabe quantas vezes esse conteúdo foi duplicado, a não ser que se programe o conteúdo para tanto. É possível fazer uma programação que permita rastrear o conteúdo clicado ou baixado, mas aí estaríamos entrando na seara do Direito à Privacidade daquele usuário que teve contato com o conteúdo.

66. TAPSCOTT, Don. *Wikonomics*. Rio de Janeiro: Nova Fronteira, 2007.

67. A proteção contra os danos advindos de calúnia, difamação e injúria está amplamente legislada, a começar pela Constituição Federal, art. 5º, X, pelo Código Penal, arts. 138 a 140, pelo Código Civil, art. 186, pelo Código de Defesa do Consumidor, art. 6º, VI, e pela Lei de Imprensa (Lei n. 5.250/67), arts. 20 a 22.

Sendo assim, as empresas que trabalham com conteúdo na Internet devem ter cuidado redobrado com as informações que veiculam. Uma notícia errada de jornal pode ser consertada por uma errata⁶⁸ publicada na próxima edição, que será aceita como a verdade daquele dia. Uma notícia falsa divulgada pela Internet será lida como verdadeira todas as vezes em que for acessada, mesmo que seja em *sites* diferentes daquele que a divulgou originalmente e ainda que aquele a tenha excluído de todas as suas páginas. Uma vez copiada, muito provavelmente esta notícia já se espalhou inevitavelmente pelo mundo virtual.

Seduzidos pela velocidade da rede, muitos provedores de conteúdo preferem soltar uma informação sem verificá-la suficientemente, o que ocorre também no mundo real, é claro; mas, como vimos, com efeitos muitas vezes menos devastadores. Quem estiver disposto a investir em informação veloz no mundo virtual, tem de estar preparado para investir em qualidade da informação.

Para evitar problemas de responsabilidade⁶⁹, no entanto, é importante que o provedor deixe claro em contrato que não se responsabiliza pelos conteúdos enviados por seus clientes. Isso tem de estar claro para todos os usuários, parceiros, fornecedores e todos aqueles que fazem parte das relações de conteúdo. Caso contrário, fazendo uma comparação simples, o provedor estará dando ao detentor de uma conta um cheque em branco com sua assinatura, sendo responsável por onde esse “cheque” venha a cair.

No caso das empresas que comercializam conteúdos restritos, é importante atentar para o efeito multiplicador da Internet e prever, em contrato ou outro meio juridicamente legal e eficaz, que os limites de responsabilidade pelo que é divulgado valem apenas até o primeiro comprador de uma informação. O conteúdo vazado, além disso, já não será de responsabilidade da empresa, por não poder ter o controle editorial sobre ele caso venha a ser alterado por seu receptor antes de ser passado adiante novamente.

Como em qualquer relação, o nexo de causalidade da responsabilidade civil será mais claramente definido se as informações forem transparentes. Da mesma forma que ocorre no mundo real quando se publica uma biografia não

68. Art. 26, *caput*, da Lei de Imprensa (Lei n. 5.250/67): “Art. 26. *A retratação ou retificação espontânea, expressa e cabal, feita antes de iniciado o procedimento judicial, excluirá a ação penal contra o responsável pelos crimes previstos nos arts. 20 e 22*”.

69. O art. 927 do Código Civil afirma: “*Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem*”.

autorizada — a advertência está claramente expressa na capa. Na questão do conteúdo em termos comerciais, é essencial que sempre haja um responsável editorial⁷⁰ por ele, como funciona com as empresas tradicionais.

Para os veículos de comunicação, vale destacar a atenção que deve haver quanto ao modo em que são publicadas as notícias pela imprensa na Internet, algo que deve ter abordagem respaldada em princípios legais e éticos. Na esfera legal, temos a Lei de Imprensa, Lei n. 5.250/67, que é minuciosa ao tratar da responsabilidade do jornalista, regulamentando o direito de resposta, caracterizando os crimes de imprensa e estabelecendo as penalidades e indenizações cabíveis. Sabemos que a verdadeira missão da imprensa é a de difundir conhecimentos, disseminar a cultura, iluminar as consciências, canalizar as aspirações populares. Contudo, em qualquer meio de divulgação de uma informação, inclusive a Internet, deve-se ter em mente que a liberdade de imprensa deve ser limitada pelos demais direitos fundamentais. Assim, na atividade jornalística deve haver responsabilidade por parte das empresas e profissionais da área, pois a ninguém é dada a prerrogativa de quebrar a harmonia social ou expor à desonra a vida moral de seus semelhantes. Mesmo não havendo a citação da Internet entre os veículos de comunicação elencados na Lei de Imprensa, o STJ tem aceitado a aplicabilidade deste dispositivo legal para regular delitos contra a honra praticados na Internet⁷¹.

70. O art. 50 da Lei n. 5.250/67 concede às empresas que explorem conteúdos uma ação de regresso contra o autor ou responsável editorial: “Art. 50. *A empresa que explora o meio de informação ou divulgação terá ação regressiva para haver do autor do escrito, transmissão ou notícia, ou do responsável por sua divulgação, a indenização que pagar em virtude da responsabilidade prevista nesta Lei*”.

71. Nesse sentido já existem decisões como estas:

Recurso em Sentido Estrito n. 9.096-0/220 (200601550212) Comarca de Goiânia. Recorrente : A.V.S.J. 1º Recorrido : W.H.M.C.F.J. 2º Recorrido : Ministério Público. Parecerista: Dra. Maria da Conceição Rodrigues dos Santos. Relator : Juiz G. LEANDRO S. CRISPIM — EMENTA. RECURSO EM SENTIDO ESTRITO. EXCEÇÃO DE INCOMPETÊNCIA CRIMINAL. CRIME CONTRA A HONRA. INTERNET. LEI DE IMPRENSA. ANALOGIA. LITIGÂNCIA DE MÁ-FÉ. NÃO CONFIGURADO. Aos crimes contra a honra, praticados através da rede mundial de computadores — internet — aplica-se, por analogia, a Lei de Imprensa (Lei n. 5.250/67), para fins de fixação da competência territorial. Situando-se a administração do *site* que publicou a notícia caluniosa na cidade (...) — STJ — SUPERIOR TRIBUNAL DE JUSTIÇA — Classe: AGRAPN — AGRAVO REGIMENTAL DA AÇÃO PENAL — 442. Processo: 200501991675. UF: DF. Órgão Julgador: CORTE ESPECIAL. Rel. Fernando Gonçalves PENAL. INJÚRIA. PUBLICAÇÃO OFENSIVA. SITE DA INTERNET. APLICAÇÃO DA LEI DE IMPRENSA. DECADÊNCIA. EXTINÇÃO DA PUNIBILIDADE.

1 — Uma entrevista concedida em um *chat* (sala virtual de bate-papo), disponibilizada de modo “online”, na *home page* de um jornal virtual, se reveste de publicidade bastante para se sub-

Uma das soluções viáveis para a questão da infração autoral no teor do conteúdo ou na criação de conteúdos falsos, falaciosos, em nome de terceiros ou de entidades que tenham credibilidade no mercado, em termos de territorialidade, a possibilidade de aplicação das regras gerais do direito internacional quanto ao ato ilegal: o fato será julgado no país em que se originou, ou, se acordado entre as partes, fica determinado um mediador que faça a subsunção das diversas normas dos vários ordenamentos ao caso concreto, de acordo com a Lei de Introdução às Normas do Direito Brasileiro.

Não há como falar de proteção de *websites* e conteúdos na internet sem tratar da questão do *Copyright*. Para tanto, devemos fazer a leitura do art. 2º do WCT: “A proteção de *Copyright* abrange expressões e não ideias, procedimentos, métodos de operação ou conceitos matemáticos em si”.

O WCT (WIPO⁷² *Copyright Treaty*) é um tratado adotado pela OMPI⁷³ em 20 de dezembro de 1996, cuja finalidade é a proteção do trabalho literário e artístico dos países signatários da Convenção de Berna.

Embora o Brasil seja signatário da Convenção de Berna, não adotou em seu ordenamento jurídico o tratado WCT, razão pela qual o instituto de *Copyright* não é aplicado no País.

Os países signatários do WCT totalizam 58 (cinquenta e oito), dentre os quais: Reino Unido, França, Holanda, Alemanha, Itália, Japão, Coreia, Espanha, Portugal, África do Sul, Suíça, Suécia, Estados Unidos, Canadá, México, Chile, Colômbia, Uruguai, Argentina, Bolívia, Paraguai, Peru e Venezuela.

No assunto de proteção de direitos autorais na Internet, é fundamental também a compreensão do que se entende por *copyleft*, que é um trocadilho para o termo *copyright* e significa justamente “deixar copiar”. Devemos ressaltar que cabe ao titular do direito autoral, que pode ser o próprio autor ou um terceiro, como o distribuidor, definir as regras que irão reger os limites de uso e disposição dele. Isso é um direito do autor e não do consumidor do conteúdo.

Vale ainda a menção do *Creative Commons*, a mais famosa técnica de *copyleft*, que é um conjunto de licenças padronizadas de forma a permitir a fácil adoção pelos autores que querem disponibilizar o acesso às suas obras, com a expressa renúncia de parte ou de todos os seus direitos patrimoniais. A vanta-

sumir ao art. 12 da Lei n. 5.250/67 e, pois, atrair a incidência do prazo decadencial de três meses (art. 41, § 1º). Precedente da Corte (...).

72. WIPO — World Intellectual Property Organization.

73. OMPI — Organização Mundial da Propriedade Intelectual.

gem dessas licenças está na criação de padrões que permitem a fácil identificação dos limites de uso concedidos pelo autor.

Ou seja, verificamos que o direito autoral é uma das matérias jurídicas com maior quantidade de desafios para os profissionais e que devem harmonizar interesses muitas vezes conflitantes, modelos de negócio já ultrapassados e questionáveis da indústria tradicional, bem como novos modelos de negócios que desafiam os limites de responsabilidade. Entre estes, há a questão: em que momento o distribuidor de uma ferramenta multifuncional deve ser responsabilizado pelas ações ilegais de seus usuários? É o exemplo dos mecanismos *peer-to-peer* tais como Kazaa, Napster, Morpheus, eMule, Grokster etc.

No tocante aos *websites*, já é possível sua proteção legal como Obra, na Biblioteca Nacional⁷⁴. Podem ser protegidos o seu aspecto gráfico geral, a sua programação, a sua base de dados eletrônica, o seu conteúdo e a sua estrutura.

O *website* tem sido entendido como uma obra coletiva (aquela realizada por diversas pessoas, sob a organização e coordenação de uma pessoa jurídica, que é a titular dos direitos patrimoniais da obra criada) quando envolve diversas partes. Se entendido como obra coletiva, cabe analisar quem é o organizador, ou seja, o titular dos direitos patrimoniais sobre o conjunto da obra.

Quando os *websites* são produzidos por somente uma pessoa (*webdesigner*), este é considerado o autor, com direitos morais inalienáveis e irrenunciáveis.

Como proteger um *webdesigner* que teve o projeto de um *site* publicado de forma ilegal na Internet por um terceiro que tinha interesse em contratá-lo para prestar tal serviço? Que medidas poderão ser tomadas? Qualquer prova legal é válida, inclusive: a) projeto de desenvolvimento do *site*; b) provas de publicação (que o *site* foi colocado no ar); c) testemunhas; d) *e-mails* trocados com o cliente/infrator; e) documento ou registro do servidor em que as páginas foram inicialmente hospedadas ou ainda continuam acessíveis; f) local em que o *site* está alocado (domínio); g) provedor de hospedagem (se for um terceiro); h) impressão (*print screen*) da tela do *site* publicado ilegalmente; i) ata notarial.

Considerando os parágrafos acima se faz oportuna a apresentação do conceito de plágio que consiste em se publicar, como próprias, obras ou parte de obras produzidas por outrem. E conforme tipificado pelo art. 184 do Código Penal brasileiro: “violar direitos de autor e os que lhe são conexos. Pena — detenção, de 3 (três) meses a 1 (um) ano, ou multa”.

Para que se configure o tipo penal, a melhor doutrina entende que devem ser comprovados os seguintes elementos, a saber: a) anterioridade da obra

74. Biblioteca Nacional — <www.bn.br>.

plagiada; b) a semelhança no tratamento do assunto; c) traços ainda que isolados de cópia literal; d) verificar se a obra podia ter sido elaborada sem a obra antecedente; e) prova de acesso à obra original. É comum realização de perícia para determinação da presença desses indícios.

Com o advento das novas mídias, passou-se a fazer uso de uma série de ferramentas, que, dependendo como sejam aplicadas, podem gerar risco legal. Entre esses casos se encontra, por exemplo, o uso do “*Link Patrocinado*”, que pode gerar o risco de concorrência desleal, previsto pelo art. 195 da Lei n. 9.279/96⁷⁵. Isso porque se ele fizer uso de marca de terceiro, devidamente registrada, pode representar um desvio de clientela. Por isso, a definição das palavras-chave e dos links patrocinados tem de ser feita com cautela.

Logo, para concluir, o tema só tende a crescer em termos de debate e interesse, já que o maior ativo da sociedade digital é o conhecimento, e, por sua vez, o Ordenamento Jurídico passa a ser demandado para sua proteção.

8.10. Aspectos legais do *software*

A ideia de coisa incorpórea não é recente, muito pelo contrário, ela nos remete às Instituições de Gaio. Entretanto, tal conceito deve ser estendido para atingir a complexidade da sociedade digital.

Segundo as Instituições, coisa corpórea é tudo aquilo que pode ser tocado, e coisa incorpórea é o que não pode ser tocado. Cernelutti adotou tal concepção e ampliou: “*res corporalis* é coisa de existência material; *res incorporalis* é um bem de existência abstrata”⁷⁶.

75. A Lei n. 9.279/96, em seu art. 195, trata dos crimes de concorrência desleal no âmbito da proteção à propriedade industrial, *in verbis*:

“Art. 195. Comete crime de concorrência desleal quem:

I — publica, por qualquer meio, falsa afirmação, em detrimento de concorrente, com o fim de obter vantagem;

II — presta ou divulga, acerca de concorrente, falsa informação, com o fim de obter vantagem;

III — emprega meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem;

IV — usa expressão ou sinal de propaganda alheios, ou os imita, de modo a criar confusão entre os produtos ou estabelecimentos”.

OBS.: Devemos citar ainda sobre este tema a obra de Francesco Cernelutti, *Teoria geral do direito*, São Paulo: Saraiva, 1942.

76. CERNELUTTI, Francesco. *Teoria geral do direito*. São Paulo: Saraiva, 1942.

Dessa forma, *res corporalis* é o que existe no plano físico, mesmo que intangível, enquanto *res incorporalis* é o que existe no plano intelectual, mesmo que exteriorizada em um suporte físico.

O *software* é coisa incorpórea, conforme vimos acima; entretanto, outras questões pairam sobre os programas de computador.

Software é produto ou serviço? Quais são as diferenças entre *Software* Proprietário e *Software* Livre? O que é licença de *Software*? Essas são algumas das questões tratadas.

Programa é uma sequência lógica de instruções (algoritmos), escritas em linguagem de programação (computação), para serem executadas passo a passo com a finalidade de atingir determinado objetivo.

A Lei n. 9.609/98 traz a seguinte definição em seu art. 1º: “Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados”.

Algoritmo é a descrição sequencial dos passos que devem ser executados, de forma lógica, clara e em português, com a finalidade de facilitar a resolução de um problema.

As linguagens de programação são divididas em dois tipos: baixo nível (linguagem de máquina, *Assembly*, Montador, *Assembler*) e de alto nível (Delphi, C++, Java, VB).

Como o computador só executa instruções em linguagem de máquina (código binário, 0 e 1), para ele executar instruções escritas em linguagens diferentes, faz-se necessário que essas instruções sejam traduzidas para linguagem de máquina.

Existem tipos básicos de tradutores: montador (traduz linguagem *Assembly* para linguagem de máquina), e interpretador (realiza tradução e execução simultaneamente, não gerando o código objeto em disco). A geração de código em disco é observada no *run-time* e compilador. A diferença entre eles é que o *run-time* trabalha com um código intermediário (pseudocompilado) e o compilador (gera executáveis .exe) cria um código objeto independente.

A expressão “*Software* Livre” é um conceito que se refere à liberdade de usar, e não a falta de pagamento, isto é, a inexistência de contraprestação pecuniária para aquisição.

Software livre é liberdade do usuário de executar, copiar, distribuir, estudar, modificar e aperfeiçoar o programa, mais especificamente alusivo a quatro tipos de liberdade para seus usuários: a de executar o programa, para qualquer propósito; a de estudar como o programa funciona, e adaptá-lo para as suas necessidades (o acesso ao código-fonte é um pré-requisito para esta liberdade); a de redistribuir cópias de modo que você possa ajudar o seu próximo; a de aperfeiçoar o programa e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie (o acesso ao código-fonte é um pré-requisito para esta liberdade).

Um programa pode ser considerado *software* livre caso os usuários tenham todas essas liberdades. Portanto, você deve ser livre para redistribuir cópias, seja com ou sem modificações, seja de graça ou cobrando uma taxa pela distribuição, para qualquer um em qualquer lugar. Ser livre para fazer essas coisas significa (entre outras coisas) que você não tem de pedir ou pagar pela permissão.

Já “*Software* Proprietário”, além de não conferir ao usuário acesso ao código-fonte, também não permite a cópia, distribuição e aperfeiçoamento, pois não tem acesso ao código.

Nesta modalidade há contraprestação, ou seja, existe pagamento e faz-se necessária a permissão para seu uso, Licença de Uso.

O registro do *software* não é imprescindível para a proteção do direito autoral. Isso significa que a partir da exteriorização intelectual nasce o direito de autor sobre a criação, como em qualquer outra obra autoral.

O registro deve ser efetuado no INPI — Instituto Nacional da Propriedade Industrial —, instituto que possui um departamento só para registro de *software* denominado DIMAPRO (Divisão de contratos de licença de uso e registros de programas de computador).

O requerimento deve conter os dados sobre o autor do programa e do titular, se este divergir do autor; se é pessoa jurídica ou física, a identificação e descrição funcional do programa de computador e trechos do código-fonte. Estes deverão ser capazes de identificá-lo e caracterizar sua originalidade.

Tais informações são prestadas em caráter sigiloso, não podendo ser reveladas, exceto por ordem judicial ou pelo próprio titular.

O uso de um programa, em qualquer modalidade, depende de autorização prévia e expressa do titular do direito.

No Brasil tal autorização é concedida mediante contrato de licença, o qual pode ser definido como negócio jurídico que almeja regulamentar o uso de programa de computador.

Na concessão da licença de uso, a finalidade do uso está expressa no documento. A licença é uma autorização específica para determinada modalidade de uso. Permite apenas a forma de utilização constante no documento. As modalidades estão descritas na Lei de Direito Autoral, no art. 31.

Em virtude da comercialização e distribuição maciça, seria impossível celebrar um contrato com cada usuário. O titular, então, concede ao usuário um “contrato” de licença. Na realidade o termo mais correto, nesse momento, não seria contrato, pois inexistente a bilateralidade; outros termos são utilizados, como oferta ou termo.

Apesar deste fato, a licença é dispositivo capaz de autorizar o uso do *software*, pois ela é uma manifestação de vontade dentro dos parâmetros legais exigidos. Além disso, com a aceitação do termo, aí sim surge a bilateralidade do negócio jurídico. Somente depois da aceitação há criação de um contrato.

A pergunta exposta acima — *Software* é produto ou serviço? — depende de outras questões: Como é feito? Como vai ser comercializado? Há atualização ou manutenção? Dependendo, ele pode ser produto, e no caso passa a ser cobrado como *royalty*, e não há incidência de imposto, ou passa a ser serviço e então recai o ISS. Pode ainda haver a hipótese de pagamento de ICMS quando o produto fica a tal ponto de prateleira (“*software* de caixinha”) que é entendido como mercadoria.

Com relação ao *software* em si, a ISO formulou boas práticas sobre característica, avaliação, qualidade e processos do ciclo de vida. Essas são: ISO/IEC 9126 — Características da Qualidade de *Software*; ISO/IEC 14958 — Guias de Avaliação de Produto de *Software*; ISO/IEC 12119 — Requisitos de Qualidade e Testes de Pacotes de *Software*; e ISO/IEC 12207 — Processos do Ciclo de Vida do *Software*.

Quanto ao lado jurídico, apesar de não haver obrigação na formulação do registro do *software*, é bastante coerente fazê-lo. Também a licença de uso é importantíssima para o criador, pois é nesse documento que estará determinado o que o usuário pode ou não fazer com o *software*⁷⁷.

77. Ressaltamos que há hoje no mercado diversos tipos de contratação de tecnologia, sendo as mais comuns:

a) licença perpétua de aquisição — modelo que existe há quase 40 anos, utilizado por grandes fornecedores como Microsoft, SAP, Oracle, IBM, que financiam o desenvolvimento de seus sistemas e os vendem para os clientes como um ativo (o contratante tem o direito ao produto para toda vida, excluindo manutenção e atualizações, que são vendidos como serviços com taxas normalmente anuais);

Para finalizar este tópico, importa destacar a recente discussão sobre Patente de *Software*. A explanação a seguir foi elaborada em conjunto com o advogado que consideramos que mais entende de direitos autorais no Brasil, Dr. Luiz Henrique Souza, cuja carreira esta autora tem o privilégio de acompanhar desde 2001.

Em 16 de março de 2012, o Instituto Nacional da Propriedade Intelectual (INPI) abriu consulta pública sobre procedimentos para o exame de pedidos de patentes envolvendo invenções implementadas por programa de computador. O texto submetido a análise apresenta as diretrizes de exame que serão adotadas pelo INPI para auxiliar no exame técnico de pedidos de patentes referentes a invenções proporcionadas por programa de computador em conformidade com a Lei da Propriedade Industrial (LPI) n. 9.279/96, bem como com os procedimentos contidos no Ato Normativo (AN) 127/97.

Antes de analisarmos a conveniência de o país adotar um modelo de proteção de invenção baseada em *software*, é necessário explicar sobre a atual proteção jurídica do *software*. No Brasil, assim como em outros países, o *software* é objeto de uma proteção muito semelhante à do direito de autor para obras literárias artísticas e científicas. Isso significa que o conteúdo protegido

b) licença de uso — direito apenas de uso por máquina instalada (ou por usuário), incluindo atualizações (mas não há manutenção);

c) licença de manutenção — empresa paga pelas taxas de correções e de manutenção do *software* adquirido;

d) conjunto de licenças (aquisição, uso e manutenção) — é o formato mais usado atualmente no mercado, o cliente tem direito ao pacote completo de licença, uso e manutenção;

e) aluguel (ASP) — o *software* fica hospedado fora da empresa que paga uma taxa fixa (pode ser mensal ou anual);

f) *Software* como serviço (SaaS) — o usuário não precisa ter nada instalado internamente, não se preocupa onde fica o banco de dados, o sistema, os aplicativos. Tudo fica fora da empresa, o modelo é considerado uma ruptura de conceito, uma vez que não se paga nem pela aquisição do *software* nem aluguel. O valor é cobrado pelo número de usuários que acessa o serviço (pelo uso);

g) *open source* — o usuário não paga pela licença inicial, já que o *software* é livre. Embora não exista o mesmo custo de desenvolvimento, é comum a cobrança por manutenção;

h) autofinanciamento — quem paga pelo desenvolvimento é o cliente, não o desenvolvedor, já que nesse modelo a solução é customizada para atender ao interesse do contratante. O cliente é o dono do *software* e, no futuro, pode até vendê-lo a outras empresas como fornecedor (é o “sob encomenda”);

i) *co-source* — quando duas empresas se unem e dividem o custo do desenvolvimento, é um trabalho colaborativo entre cliente e fornecedor, a remuneração ocorre por resultado e ambos podem explorar o *software* (muito comum em desenvolvimento de plataforma de *e-business*).

abrange o *software* em si, na sua expressão e principalmente na literalidade do código-fonte, mas não se estabelecem condições de exclusividade com relação às funcionalidades.

Os direitos sobre *software*, como já foi dito, são regulados pela Lei n. 9.609/98, e subsidiariamente pela Lei de Direito de Autor, Lei n. 9.610/98. A patente, contudo, concede uma exclusividade sobre a invenção desenvolvida e impede que outras empresas desenvolvam produtos utilizando a mesma solução técnica.

Atualmente, apenas nos Estados Unidos e no Japão são concedidas patentes de inventos implementados por *software*. O Parlamento Europeu descartou de forma veemente esta abordagem em 2005, ao rejeitar uma diretiva sobre “Inventos Implementados por Computador”.

Existem muitos motivos para que o Brasil não estabeleça um regime de concessão de patentes para inventos baseados em *software*. Alguns deles são:

- Uma medida deste tipo deve ser introduzida por Lei Ordinária. A proposição do INPI de incorporar estas modalidades de patente pela via do Regulamento é ilegal na medida em que extrapola os limites de sua competência.

- A redação adotada pelo INPI no texto proposto à consulta é muito ampla ao permitir que quase qualquer função ou *software* seja patenteável. Na prática quase tudo o que um computador realiza poderia ser objeto de patente.

- A Patente de *Software* poderia excluir a participação dos desenvolvedores de *software* livre. Existem licenças de *software* livre que são incompatíveis com a patenteabilidade do *software* e, nesse sentido, desenvolvedores de *software* proprietário teriam maior facilidade na obtenção de patentes, o que poderia gerar uma competição injusta entre os modelos de desenvolvimento.

- Patentes de *software* são menos efetivas. Ao contrário das invenções eminentemente industriais, as patentes de *software* são em geral muito abrangentes, pouco precisas e não raro sua validade é contestada judicialmente. Mesmo nos Estados Unidos a posse de uma patente de *software* não é garantia de êxito no confronto judicial e a maioria dos casos costuma ser resolvida por meio de acordos extrajudiciais.

- A proteção do *software* conferida pelo direito de autor é efetiva, possui reconhecimento internacional e não exige nenhum registro prévio, o que a torna mais adequada às características do mercado.

Apesar das razões citadas, acreditamos que nenhum desses argumentos de lastro jurídico sequer tangencia o verdadeiro problema de o Brasil criar um sistema que permita registro de patentes de *software*.

Qualquer política de proteção à propriedade industrial deve estar baseada no interesse público de estimular a inovação e a competitividade e as patentes só se justificam em um cenário no qual a proteção da inovação é fundamental para gerar riqueza e incremento da qualidade. A premissa é a de que, quando protege o invento, o Estado estimula as empresas a investir em pesquisa e desenvolvimento para gerar soluções tecnicamente inovadoras.

O aparato jurídico de proteção às patentes também é utilizado para regular abertura de mercados e como contraprestação em acordos alfandegários. Ocorre que, no tocante à indústria de *software*, não existe nenhum interesse público na concessão de patente para esses produtos. O direito de autor tem sido mais que suficiente para estimular a criação de novos *softwares* e proteger o direito dos desenvolvedores, mantendo a competitividade, mesmo com os altos índices de pirataria dos países em desenvolvimento. Essencial ressaltar que a concessão de patentes para *software* não tem o condão de inibir a contrafação, mas sim de diminuir o número de competidores.

Este é o verdadeiro motivo pelo qual a concessão de patentes para *softwares* seria desastrosa ao país: a restrição do número de competidores e a diminuição da oferta de *softwares* que possam atuar como substitutos tornariam o mercado mais concentrado e reduziriam a concorrência entre empresas de *software*.

A criação de um sistema de patentes para *software* no Brasil provavelmente seria acompanhada de uma avalanche de pedidos oriundos de grandes empresas multinacionais, o que aniquilaria a capacidade da nossa indústria nacional e, conseqüentemente, os empregos por ela gerados.

Ao se proteger as funcionalidades dos *softwares*, cria-se uma barreira de entrada para outros desenvolvedores, que não poderiam oferecer soluções próprias para as mesmas necessidades. Assim, os desenvolvedores não disputariam mais o mercado em termos qualitativos e sim de anterioridade do pedido de patente, ou seja, independentemente da qualidade do produto.

Não existe nenhum motivo para engessarmos o mercado de *software* brasileiro, adotando um sistema de patentes que, se aplicado, só beneficiará as grandes multinacionais de *software*, num modelo que é absolutamente adverso para países em desenvolvimento.

O tratado de Panos e Vinhos, fruto de uma geopolítica determinística, foi um dos componentes de subdesenvolvimento da indústria portuguesa no início do século XVIII. Como a necessidade de artigos fabris de Portugal era muito superior à demanda inglesa de vinhos, esse desequilíbrio comercial aliado à política fiscal deixaram Portugal com um legado muito difícil de ser superado.

A história demonstra que a falta de visão sobre áreas estratégicas em períodos de revolução do setor produtivo pode ser desastrosa em longo prazo. O Brasil precisa definitivamente deixar de ser dependente da exportação de produtos primários e as patentes de *software* apenas enfraquecem a nossa capacidade competitiva.

8.11. As ferramentas de trabalho tecnológicas — correio eletrônico e outros

O correio eletrônico, apesar de muito semelhante à correspondência, é um meio de comunicação com características próprias, como número de receptores da mensagem variável e do uso para o qual está sendo submetido, se pessoal, comercial ou publicitário. Seu conteúdo é disponibilizado na rede para que seus dados sejam enviados no sistema de pacotes aleatórios, utilizando vários caminhos. Isso significa que qualquer *e-mail* pode ser lido mediante o emprego das técnicas certas e que seu sigilo e privacidade não são absolutos⁷⁸. Sendo assim, não é possível aplicar simplesmente a legislação sobre sigilo de correspondência⁷⁹ e sua proteção constitucional⁸⁰, tal como funciona atualmente. É preciso entender melhor todas as peculiaridades desse tipo de comunicação, que hoje é cada vez mais uma via de negócios.

O *e-mail* ou correio eletrônico é uma aplicação de redes de computadores, muito utilizado na Internet, que possibilita a troca de mensagens e arquivos entre os usuários. A palavra tem o significado literal de *electronic mail* ou correio eletrônico.

O *e-mail* foi criado em 1971 por um engenheiro de computação americano chamado Ray Tomlinson, por este motivo, é claro, não teria como estar

78. A Lei n. 9.296, de 24 de julho de 1996, regulamenta o inciso XII do art. 5º da Constituição Federal. “O disposto nesta Lei aplica-se à interceptação do fluxo de comunicação em sistemas de informática e telemática” (art. 1º, parágrafo único). Também existe o Projeto de Lei n. 6.503/2006, de autoria da Deputada Ann Pontes, que altera o art. 151 do Decreto-Lei n. 2.848, de 7 de dezembro de 1940 — Código Penal, tipificando como crime de violação de correspondência a violação de mensagem eletrônica.

79. Código Penal, Cap. VI — Dos Crimes Contra a Liberdade Individual, Seção III — Dos crimes contra a inviolabilidade de correspondência: “Art. 151. Devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem: Pena — detenção, de 1 (um) a 6 (seis) meses, ou multa”.

80. Constituição Federal, art. 5º, XII: “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal”.

previsto na Lei Postal Brasileira, Lei n. 6.538, que é de 1978. Desse modo, a legislação não considera o *e-mail* como uma forma de correspondência, entretanto, não se pode negar que existe uma expectativa de privacidade em tal forma de comunicação. Na visão de Mário Lobato de Paiva, “o sentido de correio é similar aos dois, porém o modo de execução é diferente”.

A questão abrange também o fato de que esse tipo de comunicação eletrônica depende de intermediadores, ou seja, receptores e transmissores que, em rede, levam a mensagem a seu destinatário final. Portanto, uma das questões jurídicas a ser considerada envolve a corresponsabilidade dos Provedores de *e-mail*⁸¹ sobre o que circula na rede. *E-mails* caluniosos podem expandir-se infinitamente. Se a origem deles for rastreada e apontar para um *e-mail* corporativo, a empresa pode ser responsabilizada legalmente pelo crime. Por isso, é importante que as empresas que disponibilizam *e-mails* corporativos deixem claro para seus funcionários qual a política de privacidade a ser adotada em relação ao seu uso: o funcionário deve saber se suas mensagens estão ou não sujeitas à monitoração⁸² da empresa. Para isso, é importante o funcionário tomar ciência por escrito do documento que trata do assunto no ato de sua contratação ou no ato da disponibilização do serviço de *e-mail* corporativo para ele, o qual deve ser cancelado e inutilizado após a saída do funcionário da empresa, para evitar mau uso ou continuidade de uso pelo próprio ou por terceiros.

81. Caso interessante, reportado na revista *Consultor Jurídico*, em 14 de setembro de 2001. O juiz Luiz Menegat, da 2ª Vara Cível de Porto Alegre — RS, determinou que o site Yahoo Brasil apontasse quem cadastrou o *e-mail* de um engenheiro no RS para que recebesse uma enorme quantidade de mensagens não autorizadas (*spam*), contendo, entre outras, ofertas de sexo e pedofilia. Processo n. 107.746.696.

82. De acordo com a decisão inédita da Primeira Turma do Tribunal Superior do Trabalho, RR 613/2000-013-10-00, Proc. TST RR-613/2000-013-10-00.7, o patrão pode sim, desde que “de forma moderada, generalizada e impessoal”, controlar as mensagens enviadas e recebidas pela caixa de correio eletrônico da empresa para obter provas para a justa causa. Foi rastreando o *e-mail* de um funcionário que o HSBC Seguros Brasil S.A. descobriu que um dos integrantes da equipe de Brasília usava o correio eletrônico corporativo para envio de fotos de mulheres nuas aos colegas. Neste caso, por unanimidade, a Primeira Turma decidiu que não houve violação à intimidade e à privacidade do empregado e que a prova é legal. O *e-mail* da empresa é ferramenta de trabalho que deve ser usada apenas para uso profissional e “não haveria qualquer intimidade a ser preservada, posto que o *e-mail* não poderia ser utilizado para fins particulares”. O ministro João Oreste Dalazen enfatizou que o correio eletrônico corporativo não pode servir para fins estritamente pessoais, para o empregado provocar prejuízo ao empregador com o envio de fotos pornográficas, por meio do computador e provedor também fornecidos pela empresa. Sabe-se que na Inglaterra tal medida já é admitida pelo ordenamento como lícita, com base na Lei RIP (*Regulation of Investigatory Power*). (Fonte: Módulo Security). Existem outras decisões, mas esta foi um divisor de águas em termos de jurisprudência. Nesse sentido, ver também o acórdão do TRT, Ac:1000708-2007-014-10-00-3 ROPS.

Um *e-mail* pessoal, portanto, tem características distintas de um *e-mail* corporativo. Um é meio de comunicação pessoal e o outro ferramenta de trabalho⁸³. Ainda, um *e-mail* comercial é juridicamente distinto de um *e-mail*

83. Jurisprudências sobre uso de *e-mail* corporativo:

O uso de mensagens de *e-mail* corporativo como prova de má conduta de empregado não fere o art. 5º (incisos X, XII e LVI) da Constituição Federal, que garante ao cidadão o direito à privacidade e sigilo de correspondências. O *e-mail* corporativo não pode ser comparado às correspondências postais e telefônicas, que possuem cunho pessoal. Ao contrário, trata-se de ferramenta disponibilizada pelo empregador — titular do poder diretivo e proprietário dos equipamentos e sistemas operados — ao empregado, para uso profissional. Esse é o entendimento da Primeira Turma do TRT da 10ª região, que confirmou sentença da lavra do juiz Cristiano Siqueira de Abreu Lima. Uma atendente telefônica recorreu à Justiça do Trabalho com o objetivo de impugnar a dispensa por justa causa que lhe foi imputada pela empresa na qual trabalhava. A alegação era de que a empresa teria usado cópias de *e-mails* para justificar a dispensa, procedimento que seria proibido pela Constituição Federal. Segundo o relator do processo, juiz Ricardo Alencar Machado, as mensagens juntadas aos autos evidenciam que a atendente de forma reiterada descumpria ordens gerais da empresa — inclusive quanto ao uso do *e-mail* corporativo para fins pessoais, que era proibido — trabalhava com extrema desídia e desrespeitava os clientes da empresa. “Procedimentos que justificam a aplicação da pena de demissão motivada — a justa causa”, ressaltou. Para o magistrado, o *e-mail* corporativo não é um benefício contratual indireto. Portanto não há como reconhecer a existência de direito à privacidade na utilização de equipamentos concebidos para a execução de funções geradas por contrato de trabalho. Os juízes da Primeira Turma concluíram que a utilização das mensagens como prova é legítima e ratificaram a demissão por justa causa. Fonte: AGEIA DENSÍ Brasil (<http://www.densi.com.br/>) em 29 de fevereiro de 2008.

TST, Ag. Instr. em RR 1130/2004-047-02-40, Rel. Min. Vieira de Mello Filho, jul. 31/10/2007. Correio eletrônico. Monitoramento. Legalidade. Não fere norma constitucional a quebra de sigilo de *e-mail* corporativo, sobretudo quando o empregador dá a seus empregados ciência prévia das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. (...) Comungo do entendimento *a quo* no sentido de afastar a alegada ofensa aos incisos X, XII, LVI do art. 5º constitucional, por não ferir norma constitucional a quebra de sigilo de *e-mail* fornecido pela empresa, sobretudo quando o empregador avisa a seus empregados acerca das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. Também o julgado recorrido consignou ter o empregador o legítimo direito de regular o uso dos bens da empresa, nos moldes do art. 2º da CLT, que prevê os poderes diretivo, regulamentar, fiscalizatório e disciplinar do empregador, inexistindo notícia acerca de excessiva conduta derivada do poder empresarial.

TRT 2, RO 01478.2004.067.02.00-6, Rel. Jane Granzoto Torres da Silva, jul. 15/09/2006. “Endereço eletrônico fornecido pelo empregador se equipara a ferramenta de trabalho e não pode ter seu uso desvirtuado pelo empregado. Pertencendo a ferramenta ao empregador, a esse cabe o acesso irrestrito, já que o empregado detém apenas sua posse.”

TRT 4, RO 01404-2004-281-04-00-1, Rel. José Felipe Ledur, jul. 25/01/2007. “... em face da prova oral, restou demonstrado o uso indevido dos equipamentos da empresa pelo reclamante em horário de trabalho, inclusive em prejuízo de sua atividade laboral, de modo que o procedimento se enquadraria nas hipóteses das alíneas ‘b’ e ‘e’ do art. 482 da CLT. (...) quando ele confirmou à depoente que tinha acessado a internet, em relação aos sites pornográficos. (...) Assim, comprovada a falta grave imputada, o empregador estava autorizado a promover a despedida do empregado por justa causa. (...)”

publicitário⁸⁴ para propaganda tipo mala-direta. Isso significa que é necessário determinar as obrigações específicas do usuário da correspondência eletrônica, dependendo da modalidade do *e-mail* que estiver utilizando, assim como o termo de concordância e responsabilidade a ser estabelecido entre as partes⁸⁵.

Uma das principais questões do uso do *e-mail* tem sido a redação adequada das mensagens corporativas. Cresceram os casos de assédio moral e sexual por meio do *e-mail* corporativo. Motivo principal? O excesso de coloquialismo. Ainda não lidamos com o *e-mail* como sendo uma prova escrita ou um papel timbrado digital. Pois bem, este é um novo cenário que as empresas estão tendo de enfrentar, pois é cada vez mais comum a relação entre chefes e subordinados ocorrer toda por escrito, com uso das ferramentas tecnológicas.

A grande questão que se coloca é: como orientar adequadamente os colaboradores, e principalmente os gestores, para que eles saibam usar de forma ética e legal o *e-mail* corporativo. Os riscos envolvendo *e-mail* corporativo não estão mais só relacionados ao mau uso para envio de conteúdo particular, como fotos, músicas, filmes, mas sim a própria redação dos *e-mails*, e agora com os celulares mais inteligentes, a redação de torpedos e demais tipos de mensagens, agora com o uso das redes sociais, que normalmente estão relacionadas a ordens e tomadas de decisão de executivos cada vez mais em mobilidade.

É preciso atualizar com urgência o Código de Ética Profissional, para vislumbrar estas novas situações e cenários, e, assim, evitar incidentes e contingências legais.

TST, Ag. Instr. em RR 2771/2003-262-02-40, Rel. Min. Maria de Assis Calsing, jul. 02/04/2008) — os dois trechos são da mesma jurisprudência. “O caso em espécie é de descoberta acidental pelo empregador que a Autora cometera falta gravíssima, contrariando expresso dispositivo do contrato de trabalho, avençado por escrito, e repassava segredos comerciais da Reclamada para empresa concorrente. (...) Como assistente de importação e exportação detinha conhecimentos de segredos estratégicos e táticos da empresa. E tinha compromisso expresso de sigilo. E de tanto não se preocupou ao ceder, sem permissão, os dados que dispunha em razão do cargo ocupado. (...) Com os fundamentos supra dou provimento ao apelo da Reclamada para considerar justa a demissão tendo em vista a gravidade da falta cometida. (...)”

84. Contra o recebimento de inúmeras mensagens indesejadas o advogado João de Campos Corrêa, de Campo Grande — MS, entrou com ações de indenização contra várias empresas. A primeira delas resultou num acordo que garantirá R\$ 800,00 por *e-mail* recebido, em troca da não divulgação do nome da empresa. O autor afirma que o Código de Defesa do Consumidor está sendo ferido quando o nome de um internauta é inserido numa lista sem nenhum consentimento (Revista *Consultor Jurídico*, 28-6-2001).

85. Já está em vigor nos Estados Unidos, desde 1º de janeiro de 2000, o “*Uniform Electronic Transactions Act*”, que concede à assinatura digital o mesmo *status* legal da assinatura em papel e torna possível a realização de contratos via *e-mail*.

A questão do assédio moral e do assédio sexual é muito nova do ponto de vista de doutrina e jurisprudência. Como definir claramente o que é “perseguição” em nível de trabalho. Até onde vai o poder disciplinar, hierárquico do empregador? Pois, com os diálogos entre chefes e subordinados cada vez mais documentados por escrito, em *e-mails*, tem-se aumentado os casos em que se o empregado faz acusação de má conduta de seu superior. Mas será que é isso mesmo ou há um certo exagero? Afinal, as máquinas não conseguem traduzir contexto, mas ficam as palavras escritas, o que, por certo, tem um grande peso do ponto de vista de prova.

Para exemplificar, apresentamos este julgado em que o servidor foi acusado por subordinada de enviar-lhe mensagens de cunho sensual e o tribunal determinou que o uso irregular de correio eletrônico é causa suficiente para processo disciplinar contra servidor. “*EMENTA: AGRADO DE INSTRUMENTO. PROCESSO ADMINISTRATIVO DISCIPLINAR. LEGALIDADE. USO INADEQUADO DE CORREIO ELETRÔNICO. CONTEÚDO IMPRÓPRIO. ADEQUAÇÃO DA SANÇÃO. (...) O julgamento acerca do conteúdo do e-mail enviado pelo AFTN através do correio eletrônico da SRF, estribou-se no padrão sociomoral do homem médio, reputando, de modo plenamente plausível, ofensivas as manifestações ali contidas*”. (TRF4, Agravo de Instrumento n. 2005.04.01.000282-9/RS)

O que se vê é que faltam parâmetros que delimitem claramente até onde deve ir a conduta sem riscos. Agir com excesso de severidade tem sido questionado cada vez mais. É preciso refletir profundamente sobre o que é a divisão social do trabalho, e voltar às origens dos grandes doutrinadores sobre o tema, chegando aos gregos que bem trataram da discussão entre “bem e mal”. Neste tema há um conflito natural entre a proteção dos direitos da personalidade (que envolve imagem, reputação, vida privada) e os poderes do empregador.

Nos últimos anos cresceu o uso do correio eletrônico, bem como da própria Internet. As empresas já possuem colaboradores que são da geração Y, nascidos a partir de 1980, totalmente dependentes de computador, Internet, celular e, agora, das redes sociais.

Apesar de ser rotina no dia a dia de trabalho, e também na vida digital, o uso de ambientes de redes sociais, comunicadores instantâneos, SMS (torpedos), fóruns de discussão *online*, chats etc., ainda há uma grande deficiência no tocante à aplicação do comportamento seguro. Ou seja, muito dos incidentes envolvendo pessoas em redes sociais estão relacionados com a falta de postura e prevenção.

Essa nova geração de profissionais nascidos e criados com a tecnologia não foi ensinada a ter um comportamento seguro dentro das redes sociais.

Por isso, é necessário conscientizar e criar um hábito de segurança digital, não apenas para não se tornarem vítimas, mas principalmente para não serem infratores, mesmo sem intenção. Por exemplo, falar mal de um chefe ou colega de trabalho pode causar problemas, pois a sociedade digital é formada por provas eletrônicas, onde documentamos muito mais nossos atos, tudo por escrito, com testemunhas-máquinas, publicado para o mundo ver em tempo real.

A melhor doutrina assevera que para configurar o assédio moral tem de haver conduta continuada e reiterada. O assédio sexual tem grande proximidade do assédio moral, visto que para ser tipificado exige que seja vertical (de superior para subordinado) e que haja contato físico. Logo, brincadeiras verbais, sem contato físico, acabam tipificando o assédio moral.

Tem sido comum o assédio moral acabar impregnando-se na cultura da empresa, cada vez mais competitiva, assim como ocorre o problema de acidente de trabalho em caráter estrutural, dentro da organização. Por isso, a documentação de prevenção é essencial para proteção da empresa, para demonstrar que não é algo intrínseco ao próprio ambiente de trabalho, que há orientação clara sobre a postura a ser tomada.

A cultura de prevenção e de postura ética no ambiente de trabalho deve vir de cima para baixo, deliberada em conjunto, pois isso evita riscos jurídicos que geram impacto financeiro. Talvez a melhor recomendação seja *“não fazer aos outros o que não gostaria que fizesse para si próprio”*. Ou seja, o Direito Digital retorna à base da moral e da ética para fazer a releitura das leis nesta nova realidade⁸⁶.

86. Lista de cuidados ao usar e-mail, Internet e celular corporativo:

O que evitar	Mais algumas dicas:
• Evite termos coloquiais, o uso de tratamento formal evita situações de subjetividade e eventuais confusões geradas por causa do uso de tratamento mais íntimo em situação de trabalho/profissional.	O tratamento mínimo deve ser Senhor (Sr.) ou Senhora (Sra.), e não “você”, independentemente do cargo. Se possível deve ser feito uso da 1ª pessoa do plural (ex.: “nós gostaríamos de saber”, “vamos agendar”), visto que a comunicação é em nome da empresa, e não uso da 1ª pessoa do singular (ex.: “eu gostaria”).
• Evite o uso de expressões como “beijos” ao final.	O correto é enviar saudações ou abraços.

8.12. Segurança da Informação e as ISOs 27002, 18044 e 27001

A questão da segurança é um dos principais temas a serem discutidos e resolvidos não apenas no Direito Digital, mas na sociedade como um todo, uma vez que é uma das barreiras para o maior aproveitamento das novas tecnologias e um limitador para a exploração de seu potencial comercial. Como já vimos, a necessidade de segurança nas expectativas da sociedade foi um dos fatores que motivaram a criação do próprio Direito como fenômeno de controle das condutas, e do Estado como ente autorizado a praticar o controle dentro de limites permitidos pela própria sociedade por meio das leis — o chamado Estado de Direito. Por isso, é lógico imaginar que toda nova tecnologia que possibilite uma nova ferramenta de relacionamento necessite de um estudo mais profundo sobre a sua capacidade em transmitir segurança e ter no Direito um mecanismo que possa garanti-la.

Mesmo que a Internet e as ferramentas tecnológicas já não sejam tão novas, ainda não está claro o que é “certo e errado” para as pessoas de um modo

• Tente tratar de assuntos gerais de modo discreto e bem-educado.	Pode-se perguntar como foi o final de semana, desejar um bom-dia, felicidades, parabéns, manifestar condolências ou pesar, mas devem-se evitar assuntos muito íntimos, que possam gerar algum tipo de constrangimento (ex.: questões médicas ou familiares).
• Evite o uso de elogios que possam gerar algum tipo de duplo sentido.	Pode-se congratular a pessoa por motivo de êxito em tarefas, mas devem-se evitar elogios que possam estar relacionados a apresentação física ou partes do corpo como “linda(o)”, “bonita(o)”, “estonteante”, “maravilhosa(o)” e outros similares.
• Evite convidar para situações “a dois” pessoas que sejam subordinados hierárquicos.	O convite para jantar, para um “encontro”, para uma situação de <i>happy hour</i> (que não seja para toda equipe) pode gerar situação de constrangimento e dar a entender eventual assédio moral.
• Evite falar mal da empresa, de pessoas do trabalho, principalmente com uso de expressões pejorativas, associação com animais, gozação, piada com uso de características físicas ou emocionais.	Deve-se lembrar que o ambiente corporativo é monitorado, por isso, intrigas, uso de palavras para denegrir a imagem de um colega ou chefe podem gerar muitos problemas, e, como está por escrito, fica difícil alegar que “não era bem o que queria dizer”.

geral. Já que em uma empresa tais ferramentas devem ser usadas para finalidade de trabalho, cabe a ela definir com Políticas e com diretrizes de Segurança da Informação o que é mais adequado para proteção do negócio e dos empregados, evitando que se corram riscos desnecessários que possam gerar responsabilidade civil, criminal e até demissão.

Mas o que é informação como ativo? Segundo Marcos Sêmola “a informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para continuidade operacional e saúde da empresa⁸⁷”. Dessa forma, é importante destacar que a Informação é da Empresa e não daquele que a manipula.

Entendendo a informação como ativo intangível é possível deduzir que esteja sujeita a diversas ameaças, tais como: acesso indevido, furto de informações; fraude eletrônica e falsificação de identidade; dano aos dados e informações arquivadas; espionagem para obtenção de segredos industriais/comerciais; cópia de programa; violação do direito autoral; interceptação indevida de informação; violação de bases de dados pessoais; uso indevido de marca em *Search Engine* para gerar tráfego; exposição da marca associada a conteúdo ofensivo ou falso em *Chat, Newsgroup, Messaging, Peer-To-Peer Network, Streaming Midia, e-mail, Website, Hotsite, “Sucks” Sites* — frustração do consumidor — atualmente também em Comunidades, *Blogs, Fotologs, Forums*; Pirataria — de marca, texto, áudio, vídeo, música, *software*; pornografia.

Diante deste cenário surge a norma ISO/IEC 27002 (antiga 17799:2005), segundo a qual segurança da informação “é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”⁸⁸.

A principal causa para o vazamento de informações são as próprias ações humanas. Com propriedade, o autor Antônio Everardo Nunes da Silva⁸⁹ destaca que a falha humana é o principal motivo para darmos maior atenção à Segurança da Informação. Mesmo dentro do ambiente corporativo, ou até mesmo dentro da própria residência, é necessário ter cautela com os ativos e informações que são suscetíveis de vazamento. Dessa forma, devemos estar cada vez mais atentos e conscientes de que a informação é a moeda mais preciosa na era do conhecimento.

87. *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Elsevier, 2003. p. 9.

88. ISO/IEC 27002.

89. SILVA, Antônio Everardo Nunes da. *Segurança da informação, vazamento de informações*. As informações estão realmente seguras em sua empresa? Editora Ciência Moderna.

Quanto aos seus objetivos, a Segurança da Informação visa a três pontos: a) confidencialidade — a informação só deve ser acessada por quem de direito; b) integridade — evitar que os dados sejam apagados ou alterados sem a devida autorização do proprietário; e c) disponibilidade — as informações devem sempre estar disponíveis para acesso. Alguns autores defendem o acréscimo de mais dois aspectos: a autenticidade e a legalidade⁹⁰.

A autenticidade é a capacidade de identificar e reconhecer formalmente a identidade dos elementos de uma comunicação eletrônica ou comércio. Já a legalidade é “*característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes*”⁹¹.

De acordo com a norma ISO/IEC 27002 (antiga 17799:2005), para realizar um projeto de segurança da informação o primeiro passo é inventariar todos os ativos — fazer uma análise de risco (qualitativa e quantitativa), de maneira que se possa descobrir quais são suas vulnerabilidades. Em seguida devem ser classificadas as informações de acordo com sua sensibilidade e criticidade, considerando a seguinte divisão pública, privada e confidencial. Nesse mesmo período é recomendável a criação do Comitê de Segurança da Empresa, o qual deverá ser formado por membros da organização de diversas áreas.

Após esses primeiros passos, deve-se iniciar a elaboração da Política de Segurança. Tal documento deve conter todas as diretrizes sobre segurança da empresa, de acordo com sua própria cultura, ou seja, usar a regra do jogo no próprio jogo, estabelecendo controles de acesso físicos (segurança física) e lógicos (segurança rede).

Todos os controles que forem implementados devem ser testados, ou seja, deve ser auditado tudo o que tenha sido implementado ou não para se criar um plano de contingência que permita agir em situação de falha de algum processo. A criação deste plano de gestão da segurança da informação não é nada simples. É preciso harmonizar uma série de fatores, que vão de

90. Alguns autores usam o conceito de irretratabilidade em vez de legalidade; para nós, o de legalidade é mais amplo e abrangente e a Segurança da Informação deve estar em conformidade legal. Nem sempre isso vai significar uma obrigação irretratável, pois não diz respeito apenas ao repúdio ou impugnação de provas, mas às situações de fato e de direito envolvidas caso a caso.

91. SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. Rio de Janeiro: Elsevier, 2003. p. 46.

aspectos técnicos, no sentido de implementação de *softwares* e *hardwares* para segurança da informação, aos aspectos jurídicos, em especial a aplicação de monitoramento⁹² que não gere riscos legais de privacidade, ou infrações civil e penal.

Os principais objetivos da criação da Política da Segurança da Informação são: a) adequar o sistema de controles à crescente complexidade operacional; b) reduzir os riscos de descontinuidade, parcial ou total, da operação; c) reduzir os riscos de vazamentos de segredos do negócio; d) reduzir os riscos de fraudes; e) reduzir os riscos de não cumprimento de obrigações legais; f) atender às recomendações da auditoria externa; g) adequar o sistema de gestão de riscos em TI aos padrões de mercado; h) formalizar papéis e responsabilidades de todos os colaboradores; i) comunicar formalmente o que é permitido ou proibido em

92. Dicas para fazer monitoramento corporativo sem riscos legais:

- evitar subjetividade e/ou generalizações;
- deixar claro o conceito de identidade digital (não apenas de senhas) e alinhar com alçadas e poderes;
- deixar claro que há monitoramento (e prever as duas hipóteses tanto para fins de segurança como de produtividade);
- deixar claro que há inspeção física de equipamentos da empresa, particulares e/ou de terceiros;
- deixar claro que os recursos devem ser usados só para fins profissionais;
- prever que a mera tentativa de burlar também é uma infração às normas;
- deixar clara proibição de infração de direitos autorais, prática de pirataria, pornografia, pedofilia, guarda, manuseio de conteúdos ilícitos ou de origem duvidosa e que a empresa vai colaborar com as autoridades;
- tratar sobre a má conduta (infração mais ética do que jurídica);
- prever a divulgação da norma;
- deixar claro papéis e responsabilidades;
- definir aplicabilidade;
- gerar assinatura física e/ou eletrônica do termo de ciência;
- deixar claro que é a empresa que detém a propriedade dos recursos, bem como direitos autorais das criações e demais proteções de ativos intangíveis;
- reforçar o dever de confidencialidade e sigilo;
- determinar a possibilidade de processo disciplinar;
- determinar requisito de inserção de cláusulas específicas em contratos (se possível, atualizar contrato de trabalho para prever monitoramento);
- prever procedimento de resposta a incidentes de SI (como coletar as provas sem cometer infração a privacidade ou crime de interceptação);
- tratar da questão da mobilidade;
- implementar vacinas legais (avisos) nas próprias interfaces gráficas.

relação à manipulação de informações e uso de sistemas da empresa; j) informar que o não cumprimento da política poderá gerar punições e até mesmo a demissão por justa causa; k) servir como diretriz para que todas as áreas da organização revejam seus procedimentos, sistemas, ativos de informação e serviços prestados com o objetivo de tornarem-se conformes à nova política.

Ressaltamos que a Política de Segurança da Informação é um documento jurídico no modelo de Diretriz que traz todas as regras, padrões e procedimentos obrigatórios para proteção dos ativos e atividades da empresa, cada vez mais dependentes da informática, da Internet, do *e-mail*.

Portanto, é essencial que a empresa esteja em conformidade com a legislação e com as normas de padronização (que ajudam a suprir eventuais lacunas técnicas), devendo, neste caso, atender a ISO/IEC 27001:2005, que trata dos procedimentos e recomendações sobre Sistemas de Gestão de Segurança da Informação; a ISO/IEC 27002:2005, que estabelece um Código de Práticas para Gestão da Segurança da Informação; a ISO/IEC 18044:2004, que dispõe sobre gestão dos incidentes de segurança da informação, a norma ABNT NBR 15999, que versa sobre a Gestão de Continuidade de Negócios; a ISO/DIS 31000:2008, sobre a Gestão de Risco, a ABNT ISO/IEC 20000, sobre Gerenciamento de Serviços a legislação e tratados internacionais como a Sarbanes-Oxley, a Basileia II, e, finalmente, a legislação pátria, como a Constituição Federal de 1988, os Códigos Civil e Penal, e demais leis atualmente em vigor.

Assim sendo, os principais focos jurídicos da Segurança da Informação são: a) estar em conformidade com as leis vigentes; b) proteger a empresa de riscos e contingências legais relacionados ao mau uso da informação, ao uso não autorizado, o vazamento de informação confidencial, danos a terceiros, crime e fraude eletrônica, invasão de privacidade etc.; c) atender aos preceitos da Constituição Federal, do Código Civil, do Código Penal, da Lei de Direitos Autorais, da Lei de *Software* (antipirataria), da Consolidação das Leis do Trabalho e outros dispositivos legais nacionais e internacionais; d) garantir que, na hipótese de investigação de um incidente, a empresa possa usar as provas coletadas, e que, de forma preventiva, possa praticar monitoramento, sem que isso gere riscos legais; e) garantir que os contratos estejam adequados no tocante às responsabilidades relacionadas aos níveis de serviço acordados e aos termos de confidencialidade exigidos; f) fazer com que o time de resposta a incidentes atue com segurança jurídica, ou seja, com legitimidade jurídica.

Todos os colaboradores devem ser responsáveis por cumprir a Política de Segurança da Informação da empresa, e para tanto é necessário haver ciência formal do documento, seja com assinatura física, seja com a eletrônica. Além

disso, a etapa de divulgação e conscientização dessa Política é fundamental, tanto para prevenção de incidentes como para proteção da empresa no sentido de que capacitou seus profissionais no correto uso da tecnologia. Logo, estes serão responsáveis por seu mau uso.

A Política de Segurança da Informação (normalmente chamada de PSI) deve vir acompanhada de uma série de normas específicas que detalham o aspecto operacional de sua execução. Alguns exemplos dessas normas são: Norma de Identidade dos Usuários e Senhas, Norma de Proteção Física dos Ativos de Informação, Norma de Uso e Administração de Rede Interna, Norma de Uso de Computadores e Dispositivos da Empresa, Norma de Uso de Correio Eletrônico (*E-mail*), Norma de Uso de Internet, Norma de Uso de Dispositivos Móveis e Mídias, Norma de Classificação da Informação e Gestão Documental, Norma de Assinatura e Certificação Digital, Norma de Impressão, Cópia e Digitalização de Documentos, Norma de Geração e Preservação de Evidências, Norma de Infrações e Penalidades, Norma de Acesso Remoto à Rede, Termo ou Acordo de Confidencialidade Padrão, Termo de Responsabilidade etc.

A PSI deve ser aplicada por meio de um Comitê de Segurança da Informação, formalmente constituído, como dito, e composto por profissionais de diversas áreas. Inicialmente devem ser feitas apenas advertências aos funcionários que tiverem conduta inadequada, para que possam adequar-se, dando-se um período de transição, para que as novas regras sejam compreendidas, o qual pode variar de acordo com a realidade de cada empresa (dependendo o período pode ser de pelo menos 90 dias, no qual são apenas feitos avisos de conformidade ou não à PSI e após iniciam-se as advertências e demais procedimentos de sanção previstos e/ou aplicáveis).

Casos mais graves, como o vazamento de informação confidencial, o envio de correntes e boatos com o *e-mail* da empresa, entre outros, devem ser analisados conforme o caso, pelo Comitê de Segurança da Informação. Na verdade, nenhuma empresa quer punir: o ideal é educar e evitar riscos e responsabilidades legais para os funcionários e a empresa — por isso a importância de se fazer campanha de conscientização. A prevenção protege a todos e é a melhor medida para minimizar contingências.

A falha na segurança, na grande maioria das vezes, irá ocorrer no local mais fraco e vulnerável. Geralmente essa vulnerabilidade são os próprios usuários do sistema. Então, a empresa deve empenhar muito esforço para divulgar a PSI e fazer com que seus empregados e colaboradores tenham conhecimento desse instrumento. Não adianta apenas as equipes internas estarem cientes, é fundamental dar um tratamento específico para os terceirizados.

Outra questão que merece análise e que se tem tornado bem comum nas empresas é a criação de times internos de resposta a incidentes. Tais times são constituídos por profissionais da área técnica, Informática e redes e têm por finalidade justamente conter ou eliminar qualquer incidente de segurança da informação.

Existe um time de resposta a incidentes responsável pela Internet brasileira: é o CERT — BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil). Este Centro é mantido pelo Comitê Gestor da Internet no Brasil e, segundo descrito em seu próprio *site*, é de sua responsabilidade receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet no território nacional.

Este conceito de time de resposta a incidentes teve origem nas instalações militares americanas; depois passou a ser adotado pelo Governo americano e espalhou-se mundo afora.

Hoje, devido à importância dos ativos informacionais para as empresas, recomenda-se, para atender a necessidade de resposta rápida e imediata no momento do incidente, que cada empresa tenha seu time interno de resposta a incidentes. Dois fatores levam a tomar tal medida: 1) o tempo para responder aos incidentes é fator essencial para minimizar ou eliminar o dano que iria ser causado; e 2) geralmente as informações manuseadas por esses profissionais são extremamente sensíveis.

Considerando o foco tecnológico da Segurança da Informação, entendemos que o Direito Digital deve interpretar de forma clara o conjunto de conceitos técnicos para que possa suportar metodologias que tenham eficiência jurídica. É por isso que devemos estudar como operam, por exemplo, os mecanismos de chaves criptográficas e criptografia assimétrica. Ou seja, é preciso que o advogado tenha um mínimo de conhecimento técnico da matéria para melhor poder aplicar soluções jurídicas adequadas.

No quesito segurança, o sistema de chaves “públicas” e “privadas”, além de garantir o sigilo das transações ocorridas na rede, possibilita a identificação do remetente e do receptor, uma vez que é atribuída ao remetente uma chave privada, de conhecimento exclusivo deste, enquanto o destinatário deverá saber a chave pública, correspondente à chave privada do remetente, que é a única capaz de decodificar a mensagem enviada. Sendo assim, a chave privada funciona como uma assinatura eletrônica⁹³.

93. No Brasil a infraestrutura de chaves públicas foi instituída pela Medida Provisória n.

Há, ainda, outras tecnologias que devem ser compreendidas em sua concepção e funcionamento, como a de *Firewall*⁹⁴, uma barreira para entrada de invasores no sistema interno de empresas ou domicílios, pois com o crescimento da banda larga e da convergência, fica cada vez mais difícil e caro manter a porta fechada. A convergência aumenta o risco de exposição a *hackers*, crimes e fraudes em ambientes eletrônicos, porque possibilita um contato constante de todos com todas as portas. Por isso, vem se tentando utilizar Sistemas de Pagamento Seguro⁹⁵ (SPS) e Sistemas de Validação de cartões *online*⁹⁶ (SSL). É necessária uma padronização das chaves de criptografia e a exigência de um compromisso maior das empresas em manter a atualização de seus *softwares* de segurança com certa periodicidade, para que possamos viver em um ambiente virtual mais seguro.

Ainda, a discussão do item segurança na rede envolve a discussão de dois assuntos polêmicos: o anonimato e a privacidade. O direito à privacidade⁹⁷ constitui um limite natural ao direito à informação, assim como o direi-

2.200, de 28 de junho de 2001, reeditada no dia 27 de julho e 24 de agosto de 2001, cujas normas estão estabelecidas nos Decretos n. 3.587, de 5 de setembro de 2000, e n. 3.996, de 31 de outubro de 2001, este último alterado pelo Decreto n. 4.414, de 7 de outubro de 2002. Existem também vários projetos de lei que abordam diretamente o tema, por exemplo: o Anteprojeto de Lei da Ordem dos Advogados do Brasil, o Projeto de Lei n. 1.589, de 1999, e o Projeto de Lei n. 1.483, de 1999.

94. *Firewalls* são sistemas que têm como objetivo estabelecer regras e filtros de tráfego entre duas redes. Os *firewalls* são utilizados como a primeira linha de defesa contra ameaças externas a uma rede. Por ser a primeira linha de defesa, os sistemas de *firewall* devem ser cuidadosamente instalados e gerenciados. Porém a proteção não se restringe a apenas este mecanismo; a arquitetura de um *site* seguro para aplicações bancárias e comércio eletrônico deveria incluir os componentes: segmentação de rede, os já citados *firewalls*, mecanismos de autenticação, criptografia, detecção de intrusos (IDS), além de uma rígida segurança interna nos servidores (Guia de Referência sobre Ataques Via Internet, produzido pela *Internet Security Systems*, junho de 2000).

95. O Sistema de Pagamento Seguro ou SET — *Secure Electronic Transaction* — é um protocolo de transações seguras com criptografia de 1024 bits, que codifica todas as transações e faz uso de certificados digitais, tornando desnecessário o tráfego do número de cartão de crédito na rede. O SET garante que todas as partes envolvidas na transação (o portador da carteira eletrônica, o estabelecimento e as instituições financeiras) sejam reconhecidas e verificadas antes de a transação se realizar.

96. Conhecida como SSL — *Secure Socket Layer* —, essa forma de transação utiliza um canal privado criptografado e seguro, mas não prevê a autenticação do comprador. O estabelecimento, por sua vez, possui um certificado, porém não está protegido contra fraudes.

97. Direito à Privacidade está protegido na Constituição Federal de 1988, art. 5º, X e pela Convenção de Estrasburgo de 1981.

to ao anonimato⁹⁸ constitui um dificultador dos mecanismos de segurança em ambiente virtual⁹⁹.

A privacidade tem seus limites, no Direito, quando atinge interesses coletivos que se devem sobrepor ao direito individual dentro da sociedade. Sendo assim, em razão da primazia do princípio comunitário, no Direito Digital, é necessária a criação de diretrizes gerais que determinem o equilíbrio entre as relações paradoxais da proteção da privacidade, do comércio eletrônico, da publicidade e da segurança num mesmo ambiente jurídico-social.

Apesar de a Internet ter tido sua origem baseada em “anonimato”, ou seja, não houve uma preocupação inicial a respeito da necessidade de identificação dos seus usuários, até porque muitos dos serviços ofertados para gerar adesão à Internet usavam justamente o apelo do “suposto anonimato” para atrair clientes. Foi o que ocorreu com serviços de *chat*, encontros virtuais, *sites* de sexo, entre tantos outros de entretenimento virtual. No entanto, com sua evolução para um ambiente mais transacional, e com o seu uso maciço, verificou-se que o anonimato passou a ser um verdadeiro entrave para a manutenção de uma Internet mais segura para todos.

98. No Brasil a Constituição Federal veda em seu art. 5º, IV, o anonimato, sendo livre a manifestação do pensamento. Também o Projeto de Lei n. 18/2003 da Sra. Iara Bernardi veda o anonimato dos responsáveis por páginas na Internet e endereços eletrônicos registrados no País. O direito ao anonimato está previsto nos Ordenamentos alemão e italiano.

99. Sobre isso ver acórdão na íntegra da Decisão TJ-RJ 2004.002.20186, que acata a tese deste livro, conforme ementa a seguir: “Oitava Câmara Cível do Tribunal de Justiça. Agravo de Instrumento n. 2004.002.20186. Agravante: Telemar Norte Leste S.A. Agravado: Ibase Instituto Brasileiro de Análises Sociais e Econômicas. Relatora: Des. Letícia Sardas. Acórdão. AÇÃO CAUTELAR DE EXIBIÇÃO DE DOCUMENTOS. LIMINAR. INFORMAÇÃO DE DADOS CADASTRAIS. IP — INTERNET PROTOCOL. LEI GERAL DE TELECOMUNICAÇÕES. STFC — SERVIÇO DE TELEFONIA FIXA COMUTADA. INVASÃO DO SISTEMA DE INFORMAÇÃO. HACKER. ANONIMATO E PRIVACIDADE. DIREITO DO USUÁRIO. 1. A evolução da Internet, como ocorre com o desenvolvimento de qualquer inovação tecnológica, provocou uma transformação no estudo das normas jurídicas, formando o que se pode denominar de direito digital ou direito da informática, que tem o desafio de equilibrar a delicada balança em que se pesa o interesse econômico, a proteção da privacidade e o anonimato. 2. Os hackers são indivíduos que entram num sistema de informática, quebrando sistemas de segurança, para causar danos. 3. A discussão do tema segurança na rede envolve a discussão de dois assuntos polêmicos: anonimato e privacidade. Ora, o tema referente à segurança é, sem dúvida, um dos mais palpitantes e atuais a serem discutidos e resolvidos, não só no Direito Digital, mas na sociedade em geral. 4. O direito à privacidade constitui um limite natural ao direito à informação. 5. O direito ao anonimato constitui um dificultador dos mecanismos de segurança em ambiente virtual. 6. Incentivar a clandestinidade na rede significa torná-la um mundo em que ninguém é obrigado a nada, nem responsável por nada. 7. Os provedores, como portas de entrada e saída da rede, são os que têm possibilidade de averiguar os dados dos internautas que sejam seus clientes, propiciando que se investigue a prática de atos irregulares. 8. Desprovemento do Agravo de Instrumento”.

É claro que estabelecer rotinas de segurança rígidas pode esbarrar na questão da privacidade, afugentando usuários que possam sentir-se vigiados permanentemente, durante toda sua navegação. Apesar de ser um tema delicado, alguns princípios poderiam ser adotados desde já em busca de uma solução.

Quando é solicitado o registro de domínio no Brasil, o NIC.br, responsável pelo ato, exige a apresentação de CNPJ do requerente. Entretanto, pessoas físicas podem ter seus próprios *sites* hospedados em provedores de acesso, além, é claro, de ter contas de *e-mail*, sem a necessidade de uma identificação mais precisa. Isso coloca a responsabilidade sobre a identidade do usuário, num primeiro momento de contato com a rede, nas mãos dos provedores de internet (seja fixa ou *wireless*) e também de *lan houses* e cybercafés.

Uma das medidas que poderiam ser tomadas é a exigência de identificação no cadastramento dos usuários. Para isso, seria necessário ter como norma-padrão a criação de uma identidade virtual homogênea para cada um. É importante ressaltar que a identidade virtual é diferente da identidade do mundo real. Por exemplo, se uma pessoa registra uma conta de *e-mail* como “fulano-detal@provedor.com”, passa, para efeitos de Internet, a ser identificada como esse sujeito. Todos os atos que realizar na rede, que não solicitem RG ou CPF, serão identificados como sendo tomados por Fulano de Tal, mesmo que a pessoa que opere essa conta seja outra.

Como resolver esta questão de modo a aumentar a segurança das relações entre pessoas e empresas através dos meios eletrônicos, e ao mesmo tempo não inviabilizar ou onerar em demasia os Provedores? Entende-se que se eles não coletarem os dados do seu usuário, pode haver uma discussão sobre eventual facilitação, por negligência, o que gera uma responsabilidade civil. Mas independente disso, o crime terá sido cometido e a capacidade de prova de autoria, que é essencial para o exercício da Justiça, terá sido eliminada completamente.

Claro que, mesmo havendo um cadastramento mais rigoroso, podem continuar existindo falsos indivíduos, mas em uma proporção bem menor, o que já atende ao requisito de gestão de riscos nas relações em determinada comunidade que o Ordenamento Jurídico deve ter.

Devemos destacar que já há tecnologias que permitem que se identifique, por aproximação, mediante a análise do histórico de hábitos de navegação do usuário na rede, se o *e-mail* “fulanodetal@provedor.com” corresponde a Fulano de Tal pessoa física, real. Isso é um trabalho de inteligência em bancos de dados, e que deve crescer cada vez mais. Muitas empresas já traçam o perfil de seus

usuários para identificar na rede comportamentos suspeitos e ativar os mecanismos de bloqueio e contenção de um eventual incidente. É este inclusive o princípio utilizado na indústria de cartões de crédito, quando verifica “desvio de padrão de conduta” de um possível “número de cartão” que indica, então, que há probabilidade de não ser o cliente (fraude ou erro de autenticação) e assim aciona as medidas de verificação de autoria para autorização da operação.

É curioso verificar que quando há procedimentos mais automatizados para verificação de identidade, e sua confirmação, que às vezes envolve a verificação de informações, as pessoas sentem-se “invadidas em sua privacidade”. Ao invés de pensar que é para sua própria segurança, o cliente, na verdade, em geral, não quer ser de fato identificado. Mas a prevenção é essencial, é melhor verificar antes do que se dar conta depois, especialmente nesta era tão conectada e em tempo real.

Qual o caminho? Com certeza não se pode evoluir no sentido mais transacional da rede sem um aumento considerável de segurança, que exige um controle maior de identidade. Se isso vai significar conseguir associar um CPF a um Usuário da Internet, por meio do número de um IP (talvez no novo padrão do IPV6), ou com uso de outro tipo de padrão de identificação (assinatura digital ou biométrica), não sabemos, mas que é necessário é.

Por que, então, ainda não se propôs a criação de um banco de dados central que contivesse todas essas informações sobre as pessoas que trafegam na rede¹⁰⁰? Talvez o motivo, acreditamos, seja menos técnico do que financeiro. Atualmente, graças ao Decreto n. 3.724¹⁰¹ e à Lei Complementar n. 105, ambos de 10 de janeiro de 2001, as autoridades e os agentes fiscais da União, dos Estados, do Distrito Federal e dos Municípios ganharam o poder de proceder ao exame de dados e informações sigilosas de pessoas físicas e/ou jurídicas. Podemos, então, estabelecer uma relação entre o pluralismo dos bancos de dados e a dificuldade de combater a elisão fiscal, já que se houvesse uma centralização não seria possível ocultar um grande número de informações a respeito da capacidade contributiva das pessoas.

Acreditamos, por isso, que os provedores que investirem na segurança do usuário, garantindo que todas as contas de *e-mail* com determinada terminação

100. Existem diversas iniciativas internacionais nesse sentido, e algumas muito criticadas, principalmente do governo norte-americano (http://en.wikipedia.org/wiki/Information_Awareness_Office).

101. A redação do Decreto n. 3.724 foi alterada pelo Decreto n. 6.104, de abril de 2007.

É claro que estabelecer rotinas de segurança rígidas pode esbarrar na questão da privacidade, afugentando usuários que possam sentir-se vigiados permanentemente, durante toda sua navegação. Apesar de ser um tema delicado, alguns princípios poderiam ser adotados desde já em busca de uma solução.

Quando é solicitado o registro de domínio no Brasil, o NIC.br, responsável pelo ato, exige a apresentação de CNPJ do requerente. Entretanto, pessoas físicas podem ter seus próprios *sites* hospedados em provedores de acesso, além, é claro, de ter contas de *e-mail*, sem a necessidade de uma identificação mais precisa. Isso coloca a responsabilidade sobre a identidade do usuário, num primeiro momento de contato com a rede, nas mãos dos provedores de internet (seja fixa ou *wireless*) e também de *lan houses* e cybercafês.

Uma das medidas que poderiam ser tomadas é a exigência de identificação no cadastramento dos usuários. Para isso, seria necessário ter como norma-padrão a criação de uma identidade virtual homogênea para cada um. É importante ressaltar que a identidade virtual é diferente da identidade do mundo real. Por exemplo, se uma pessoa registra uma conta de *e-mail* como “fulano-detal@provedor.com”, passa, para efeitos de Internet, a ser identificada como esse sujeito. Todos os atos que realizar na rede, que não solicitem RG ou CPF, serão identificados como sendo tomados por Fulano de Tal, mesmo que a pessoa que opere essa conta seja outra.

Como resolver esta questão de modo a aumentar a segurança das relações entre pessoas e empresas através dos meios eletrônicos, e ao mesmo tempo não inviabilizar ou onerar em demasia os Provedores? Entende-se que se eles não coletarem os dados do seu usuário, pode haver uma discussão sobre eventual facilitação, por negligência, o que gera uma responsabilidade civil. Mas independente disso, o crime terá sido cometido e a capacidade de prova de autoria, que é essencial para o exercício da Justiça, terá sido eliminada completamente.

Claro que, mesmo havendo um cadastramento mais rigoroso, podem continuar existindo falsos indivíduos, mas em uma proporção bem menor, o que já atende ao requisito de gestão de riscos nas relações em determinada comunidade que o Ordenamento Jurídico deve ter.

Devemos destacar que já há tecnologias que permitem que se identifique, por aproximação, mediante a análise do histórico de hábitos de navegação do usuário na rede, se o *e-mail* “fulanodetal@provedor.com” corresponde a Fulano de Tal pessoa física, real. Isso é um trabalho de inteligência em bancos de dados, e que deve crescer cada vez mais. Muitas empresas já traçam o perfil de seus

usuários para identificar na rede comportamentos suspeitos e ativar os mecanismos de bloqueio e contenção de um eventual incidente. É este inclusive o princípio utilizado na indústria de cartões de crédito, quando verifica “desvio de padrão de conduta” de um possível “número de cartão” que indica, então, que há probabilidade de não ser o cliente (fraude ou erro de autenticação) e assim aciona as medidas de verificação de autoria para autorização da operação.

É curioso verificar que quando há procedimentos mais automatizados para verificação de identidade, e sua confirmação, que às vezes envolve a verificação de informações, as pessoas sentem-se “invadidas em sua privacidade”. Ao invés de pensar que é para sua própria segurança, o cliente, na verdade, em geral, não quer ser de fato identificado. Mas a prevenção é essencial, é melhor verificar antes do que se dar conta depois, especialmente nesta era tão conectada e em tempo real.

Qual o caminho? Com certeza não se pode evoluir no sentido mais transacional da rede sem um aumento considerável de segurança, que exige um controle maior de identidade. Se isso vai significar conseguir associar um CPF a um Usuário da Internet, por meio do número de um IP (talvez no novo padrão do IPV6), ou com uso de outro tipo de padrão de identificação (assinatura digital ou biométrica), não sabemos, mas que é necessário é.

Por que, então, ainda não se propôs a criação de um banco de dados central que contivesse todas essas informações sobre as pessoas que trafegam na rede¹⁰⁰? Talvez o motivo, acreditamos, seja menos técnico do que financeiro. Atualmente, graças ao Decreto n. 3.724¹⁰¹ e à Lei Complementar n. 105, ambos de 10 de janeiro de 2001, as autoridades e os agentes fiscais da União, dos Estados, do Distrito Federal e dos Municípios ganharam o poder de proceder ao exame de dados e informações sigilosas de pessoas físicas e/ou jurídicas. Podemos, então, estabelecer uma relação entre o pluralismo dos bancos de dados e a dificuldade de combater a elisão fiscal, já que se houvesse uma centralização não seria possível ocultar um grande número de informações a respeito da capacidade contributiva das pessoas.

Acreditamos, por isso, que os provedores que investirem na segurança do usuário, garantindo que todas as contas de *e-mail* com determinada terminação

100. Existem diversas iniciativas internacionais nesse sentido, e algumas muito criticadas, principalmente do governo norte-americano (http://en.wikipedia.org/wiki/Information_Awareness_Office).

101. A redação do Decreto n. 3.724 foi alterada pelo Decreto n. 6.104, de abril de 2007.

pertencam a indivíduos identificados e cadastrados, terão um diferencial para conquistar a confiança dos consumidores.

Essa questão nos traz a importância da definição da titularidade dos dados. No nosso ordenamento, os dados pertencem à pessoa¹⁰². Nessa condição, ela tem o direito de saber que informações a seu respeito determinado banco de dados possui. A lei consumerista garante o direito da pessoa de retificar ou complementar esses dados e permite, também, ao titular a solicitação de que não sejam utilizados em finalidades distintas daquelas para as quais foram fornecidos.

A lei define como “dados de acesso restrito” aqueles que, por sua natureza, só podem ser usados com a anuência expressa do titular, entre eles, os que se referem a raça, opiniões políticas e religiosas, crenças e ideologia, saúde física e mental, vida sexual, registros familiares e profissão. Um caminho de solução viável seria a criação de um Cadastro Nacional de Proprietários de Bancos de Dados Pessoais, onde cada banco possuísse um código de identificação que deveria estar presente e legível nos documentos de que fizessem uso. Dessa forma, a pessoa que recebe em sua casa uma mala-direta poderia saber, pelo código impresso na etiqueta, de onde vieram os dados a seu respeito. Uma medida como esta resolveria, talvez, o principal problema da correspondência eletrônica não solicitada, ou simplesmente denominada *spam*. Atualmente, devido ao envio automatizado de *e-mails*, nem é recomendável que a pessoa responda a um *spam* para pedir para ser excluído da base de envio (destinatário), pois isso pode, em muitos casos, se tornar um procedimento de confirmação de conta válida, e aí é que a pessoa começa a receber *e-mails* sem parar. Por isso, a questão de como ser feito o *opt-out* adequadamente é extremamente relevante, já que os fraudadores aproveitam-se das situações de “para deixar de receber *e-mail* clique aqui” para instalar um arquivo malicioso no equipamento do usuário.

As empresas que operam na rede, sejam elas totalmente virtuais ou extensões de empresas reais, também têm a obrigação de investir — e muito — em

102. Projeto de Lei do Senado n. 268/99 (arquivado), tratava sobre a estruturação e o uso de banco de dados sobre a pessoa e disciplina o rito processual do *habeas data*, e art. 5º, LXXII, da Constituição Federal de 1988, que trata do *habeas data*. Projeto de Lei n. 4.102/93, que regula a garantia constitucional da inviolabilidade de dados. Art. 5º, LXXII: “conceder-se-á *habeas data*”: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se preferir fazê-lo por processo sigiloso, judicial ou administrativo”.

segurança¹⁰³. Um exemplo bem simples: se alguém está numa loja do mundo

103. Ver decisão na íntegra de ação judicial que acatou a tese deste livro. Menção de alguns trechos resumidos a seguir: “*REQUERENTE, promoveu em face de SAMSUNG ELETRÔNICA DA AMAZÔNIA LTDA. E LOGÍSTICA SISTEMAS DE DISTRIBUIÇÃO S/A., ação de INDENIZAÇÃO POR DANO MORAL cumulada com pedido de PRODUÇÃO ANTECIPADA DE PROVAS. Segundo a inicial, o autor realizou contrato de compra e venda de mercadoria com a ré Samsung, na data de 30 de julho de 2003, via internet, tendo efetuado o pagamento via cartão de crédito, recebido a mercadoria na data marcada, cumprindo todos os procedimentos exigidos pela primeira demandada, com a emissão de nota fiscal pela segunda demandada. Todavia, foi surpreendido na data de 23 de julho de 2005, quando acessou o site disponível de busca, e ao digitar seu nome, depa-rou-se com os seus dados pessoais (nome completo, endereço de e-mail, endereço residencial completo, número do RG e CPF, informações sobre a compra realizada na loja virtual Samsung, forma de pagamento e produto adquirido, no site acessível pelo endereço <http://hackerfire.fdp.com.br/dados.htm>, juntamente com centenas de outros clientes da empresa Samsung, que efetuaram compras por esta via virtual. DE C I D O. Com efeito, está cabalmente demonstrado que o autor e a ré Samsung mantiveram relações comerciais em agosto de 2003, via comércio virtual, sendo o responsável pela logística utilizada a segunda ré. As demandadas também não negam que em julho de 2005 os arquivos da empresa Samsung foram invadidos por hacker, não localizado, que colocou na internet os dados pessoais de seus clientes, inclusive do autor, como número de RG, CPF, endereço residencial, número de telefone, bandeira do cartão de crédito, produto comprado no site da empresa Samsung, que poderia ser acessado por qualquer pessoa. No depoimento pessoal do autor este disse que seu nome foi retirado do Google em fevereiro de 2006. Deste modo, aplicável ao caso sub judice as lições contidas na obra Direito Digital, editora Saraiva, de Patricia Peck, páginas 37 e 146 em que dispõe: ‘O Direito Digital tem o desafio de equilibrar a difícil relação existente entre o interesse comercial, privacidade, responsabilidade e anonimato, gerada pelos novos veículos de comunicação. Esta equação só pode ser equilibrada se socialmente aceita e cobrada por meio de procedimentos de vigilância e punibilidade que devem ser determinados pelo próprio Direito Digital. Se, por um lado, cresce a cada dia o número de empresas que disputam os consumidores da Internet e, conseqüentemente, a publicidade virtual, com preenchimento de formulários e cadastros, por outro lado, cresce também o nível de conscientização dos consumidores quanto à possibilidade de aplicação do atual Código do Consumidor, que trata da matéria de utilização de informações de consumidores para fins comerciais, trazendo uma série de penalidades para quem a pratica. Logo, não há lacuna jurídica no tocante à solução da privacidade na Internet. Há, sim, falta de entendimento quanto à aplicação de leis em vigor para questões relativamente novas, que exigem interpretação da norma e sua adequação ao caso concreto. Este é um princípio fundamental para a aplicação do Direito, e, conseqüentemente, deve ser adotado também no Direito Digital. É evidente que o direito à privacidade constitui um limite natural ao direito à informação. No entanto, não há lesão a direito se houver consentimento, mesmo implícito, na hipótese em que a pessoa demonstra de algum modo interesse em divulgar aspectos da própria vida. Assim como há limites naturais ao direito à privacidade quando atinge interesses coletivos sobre o particular requer verificação caso a caso. Na questão do anonimato, podemos ressaltar que ele é relativo, uma vez que a própria tecnologia nos permite rastrear o emissor, assim como rastreamos ligações telefônicas e sinais de rádio. Portanto, a problemática do anonimato deve-se ao comportamento de muitas empresas que não encaminham as queixas para investigação policial por medo de que a repercussão da matéria possa vir a prejudicar sua imagem no tocante à segurança. E é este comportamento que faz com que não haja punição, o que contribui para o crescimento das práticas delituosas’. Para o Direito Digital, a teoria do risco tem maior aplicabilidade uma vez que, nascida na era da industrialização, vem resolver o problema de reparação do dano onde a culpa não é um elemento indispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações devido ao princípio de equilíbrio de interesses e genérica equidade. Considerando apenas a Internet, que é mídia e veículo de comunicação, seu potencial de danos indiretos é muito maior que o de danos diretos, e a possibilidade de causar prejuízo a outrem, mesmo que sem culpa, é real. Por isso, a*”

real, efetuando uma compra, e, nesse momento, essa loja é assaltada, a empresa proprietária terá sido a maior vítima do dano e também terá claras responsabilidades sobre o que tiver ocorrido com seus clientes naquele momento. Numa empresa virtual é bem diferente. Se o usuário tem seus dados cadastrais roubados durante o fechamento de uma transação virtual de comércio eletrônico, o prejuízo jamais será da “loja”. Ninguém entra numa “loja” virtual para roubar seus produtos, porque obviamente estes também são virtuais. Os ladrões da

teoria do risco atende e soluciona de modo mais adequado as questões virtuais, devendo estar muito bem associado à determinação legal de quem é o dever de prova em cada caso. No Direito Digital, a responsabilidade civil tem uma relação direta com grau de conhecimento do requerido de cada prestador de serviço e do consumidor usuário também. Nenhuma das partes pode alegar sua própria torpeza para se eximir de culpa concorrente em algumas hipóteses.’ Reza o artigo 159 do nosso Código Civil, atual artigo 927 do novo Código Civil, literalmente determina que aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito ou causar prejuízo a outrem, fica obrigado a reparar o dano. No caso dos autos, os réus garantiram na compra virtual o sigilo das informações do cliente, e portanto, inegável a ocorrência de dano moral ao autor, ante a divulgação indevida, expondo-o e facilitando a ação de pessoas inescrupulosas que poderiam usar seus dados para realizar inúmeras operações ilícitas, criando expectativa e preocupação, mesmo que tenha sido realizado por hacker, pois constitui o risco da atividade, sendo a responsabilidade dos demandados objetiva, por força do artigo 14 do Código de Defesa do Consumidor. É de se ponderar que a subtração dos valores ideais, tanto quanto o impedimento ao exercício desses mesmos valores, sempre se constitui em dano de natureza não patrimonial. Afinal, o homem, “para viver em sociedade, necessita preservar os seus valores individuais tanto quanto precisa deles para integrar-se no convívio social. E, sem dúvida, esse fato constitui-se na mais leve lesão perpetrada ao indivíduo e à própria sociedade, já que a comunidade fica desfalcada da contribuição de um de seus componentes, na medida em que ele próprio sente-se marginalizado do processo de socialização” (Clayton Reis, em Dano Moral — editora Forense, pág. 82 — 4. ed.) Concluindo, a reparação dos danos morais é um imperativo individual e social, em que se busca a compensação, porém, deve ser consubstanciada em quantia econômica significativa, que represente advertência ao lesante e à sociedade de que não se aceita o comportamento assumido. Ademais, não é necessário que tenha ficado caracterizada a lesão ao patrimônio do autor, pois o direito à reparação nasce do próprio ato, ou seja, ‘não se reclama, à configuração do prejuízo, o reflexo patrimonial, sendo suficiente que o fato acarrete constrangimento ao ofendido, em sede de transtornos e reações constrangedoras ...’ (neste sentido RT 772/257 — rel. Evaldo Veríssimo), o que está cabalmente demonstrado nos autos. No tocante à ausência de parâmetros para a fixação do quantum indenizatório, a jurisprudência dominante tem deixado ao arbítrio do juiz, valendo-se de seu bom senso, sentido de equidade, procurando sempre estabelecer o equilíbrio social, rompida pela ação de agentes, na prática dos atos ilícitos (neste sentido Clayton Reis, in obra citada, pág. 103). Por todo o explanado, levando-se em conta a qualificação das partes, a gravidade e conduta destas, a intensidade do dano, estando patenteado ter suportado o demandante prejuízos de ordem moral, bem como o período em que o nome do autor permaneceu indevidamente na internet estabelece-se a indenização no valor de R\$ 7.000,00 (sete mil reais), a qual servirá, para o autor como compensação pelo desconforto sofrido, e, em relação às rés como alerta, para evitar transtornos aos seus clientes. Ante o exposto, e pelo mais que dos autos consta, hei por bem julgar PROCEDENTE a ação, com fundamento no artigo 269, inciso I, do Código de Processo Civil, para condenar as rés a pagar ao autor a importância de R\$ 7.000,00 (sete mil reais), sujeito a correção monetária a partir da propositura da ação, mais juros moratórios legais desde a citação. Custas, despesas processuais e honorários advocatícios serão suportados pelas rés, arbitrados em 10% da condenação. P.R.I. São Paulo, 24 de novembro de 2006. CRISTIANE SAMPÃO ALVES MASCARI BONILHA JUÍZA DE DIREITO”.

rede visam sempre o furto de informações ou de crédito, nesse caso do usuário-cliente. Então, o maior prejudicado pela falta de segurança em *sites* desse tipo será sempre o usuário¹⁰⁴.

Logo, isso explica por que a maioria das empresas virtuais que sofrem invasões não denuncia a ocorrência, haja vista que os dados furtados são de seus “clientes” e muitas vezes serão utilizados por terceiros sem que estes percebam, pelo menos até que algo pior ocorra, principalmente no tocante ao cartão de crédito. Alguns têm medo de tornar a ocorrência pública por temerem que haja dano à marca, que passaria a imagem de ser insegura perante o universo de consumidores. Esse comportamento impõe que se tenha uma norma-padrão sobre a exigência de identificação clara de selos de segurança nesses *sites*, supervisionados periodicamente, já que a tecnologia de segurança deve ser atualizada constantemente, na mesma velocidade em que são aprimoradas as técnicas criminosas para burlá-las.

Algumas empresas assumem que têm seus sistemas penetrados por invasores constantemente, mas que estão vigilantes e conseguem deter esses invasores na superfície, antes de qualquer dano. Tal postura, na verdade, deve gerar mais confiança dos usuários, já que não existe sistema totalmente inviolável. Um *site* que se anuncia como 100% seguro é que deve ser visto com desconfiança.

Em qualquer situação de insegurança na Internet, o maior lesado é o usuário, com danos diretos e indiretos, já que ser contaminado por um vírus em um *website* ou em uma operação eletrônica pode gerar prejuízos muito maiores e mais duradouros.

É importante ressaltar que, se forem adotados padrões de segurança adequados, o ambiente virtual se torna muito mais seguro que o mundo real. A tecnologia permite que se rastreiem as ações na rede com maior precisão do que no mundo real, onde é possível desaparecer sem deixar vestígios. Toda ação no mundo virtual deixa um rastro, que pode ser seguido até a sua origem.

104. Comete um terrível erro estratégico o *site* de vendas que, pensando dessa forma, enfraquece a proteção contra ataques, primeiro porque a vantagem financeira é apenas um dos vários motivos para os ataques que podem ser também, segundo pesquisas, por vingança de funcionários descontentes e ex-funcionários, por busca de promoção e prestígio para o *cracker*, por idealismo (contra determinadas instituições) etc.; e depois, no caso de um ataque do tipo “Denial of Service” em que o *site* fica fora do ar, quanto a instituição deixa de ganhar? Sua imagem não fica arranhada? Será que não perderá clientes? É de fundamental importância para as empresas que a Internet seja encarada como um ambiente seguro para realização de atos de comércio. Portanto, fica claro que as empresas virtuais é que são as maiores interessadas na questão da segurança na rede.

Com a expansão da banda larga e da convergência, a tendência de maior número de pessoas estarem totalmente conectadas crescerá. Por isso que é obrigação do ordenamento jurídico determinar quem assume a responsabilidade pela segurança e privacidade desses indivíduos¹⁰⁵. Incentivar a clandestinidade na rede significa torná-la um mundo em que ninguém é obrigado a nada, nem responsável por nada. Ora, o dever de verificação sobre a veracidade dos dados apresentados por um cliente é da empresa que o aceita. Por isso, repetimos, os provedores, como portas de entrada e saída da rede, são os que têm maior possibilidade de averiguar os dados dos internautas que sejam seus clientes, possibilitando uma perícia que consiga investigar atos irregulares¹⁰⁶ tomados por estes.

A sociedade digital não pode eximir-se da responsabilidade de exigir que as empresas virtuais operem dentro de padrões rígidos de segurança, utilizando

105. As novas tecnologias como Internet móvel em aparelhos celulares possuem uma peculiaridade no quesito segurança: o usuário é incapaz de estabelecer rotinas de segurança em seu sistema contra invasores: não é possível, por exemplo, a implementação de um *firewall*, ou simplesmente checar se uma mensagem recebida contém um vírus. Acreditamos que as empresas que disponibilizam esses serviços têm responsabilidade objetiva pela segurança dos serviços que prestam e pelos possíveis danos causados aos consumidores, assim regulamenta o Código de Defesa do Consumidor, arts. 12 e seguintes. No entanto, o que observamos é exatamente o contrário. As empresas de telefonia móvel e os provedores quando se manifestam a respeito da segurança dos dados do usuário enquanto se utilizam dos serviços, é sempre no sentido de total exclusão de responsabilidade. Seleccionamos alguns trechos de um "aviso legal" disponibilizado pelo Terra Celular (www.terra.com.br/celular/), que presta serviços e fornece conteúdo ao usuário:

"TERRA não garante a privacidade e segurança na utilização do Portal e dos Serviços e, em particular, não garante que terceiros não autorizados possam ter conhecimento da classe, condições, características e circunstâncias de uso que os Usuários fazem do Portal e através dos Serviços".

"TERRA se exime de toda responsabilidade permitida pelo ordenamento jurídico pelos danos e prejuízos de toda natureza que possam decorrer do conhecimento que terceiros não autorizados possam ter da classe, condições, características e circunstâncias de uso que os usuários fazem do portal ou dos serviços."

"O TERRA não garante a ausência de vírus nos Conteúdos, bem como de outros elementos nocivos que possam produzir alterações em seu sistema informático (software e hardware) ou nos documentos eletrônicos e arquivos armazenados em seu sistema informático."

Essas cláusulas são claramente abusivas e estão previstas no art. 51, I, do Código de Defesa do Consumidor; são, portanto, nulas de pleno direito.

106. Sobre este tema versam dois Projetos de Lei, o n. 3.016, de 2000, do Deputado Antônio Carlos Pannunzio, e o n. 3.891, de 2000, do Sr. Júlio Semeghini. Ambos dispõem sobre o registro de informações dos usuários para possível requerimento pela autoridade judiciária, porém acreditamos que a eficácia dessas leis (se aprovadas) será comprometida pelo mecanismo de sanção contido nas normas, a multa (que varia de mil a seis mil reais). Temos por certo que um mecanismo que responsabilize o provedor objetivamente, concedendo a este ação de regresso contra o autor de um possível ilícito, seria forte o bastante para obrigar os provedores a monitorar seus clientes e manter um registro mais completo e duradouro do que o exigido na lei.

o poder da decisão de consumo como ferramenta para obrigar as empresas a se adequarem a essa nova realidade e a investirem no bem-estar de seus clientes.

Quanto à questão das Provas, assunto que será discutido em momento mais oportuno em capítulo próprio, à primeira vista, atos ocorridos na Internet não têm testemunhas. Isso é verdade se considerarmos testemunhas como pessoas humanas, físicas. Mas, no mundo virtual, as testemunhas são aqueles que armazenam os dados de navegação, são os servidores e HDs (*Hard Disk Drive*).

Por tudo exposto, a identificação mais completa e constante dos usuários, baseada em recursos de segurança mais eficazes, é a solução ideal, de modo a garantir com mais eficácia a segurança não só de uma operação, mas de toda a Internet. Visto que se o próprio princípio da Internet envolve o deslocamento de indivíduos na rede, como se fosse uma navegação, já que seus usuários estão o tempo todo entrando e saindo de diferentes lugares e países, por que não adotar o mesmo princípio que rege este tipo de situação no mundo real? Se uma pessoa viaja no mundo real, ela terá de se identificar todas as vezes em que pegar um navio, um ônibus interestadual, um avião. Esse mesmo princípio pode ser adotado no ambiente virtual, para situações que sejam previamente definidas.

Concluindo, já existem diversos projetos nacionais com propostas de nova legislação¹⁰⁷ para tratar sobre Segurança da Informação, e alguns destes já foram

107. Os projetos de lei são:

Projeto de Lei n. 2.196, de 9 de outubro de 2003: dispõe sobre a divulgação de mensagens pelos usuários de provedores na Internet e demais redes de computadores abertas ao uso do público.

Projeto de Lei n. 18, de 18 de fevereiro de 2003: veda o anonimato dos responsáveis por páginas na Internet e endereços eletrônicos registrados no País.

Projeto de Lei n. 7.093, de 6 de agosto de 2002: dispõe sobre a correspondência eletrônica comercial, e dá outras providências.

Projeto de Lei n. 3.356, de 28 de junho de 2000: dispõe sobre a oferta de serviços através de redes de informação.

Projeto de Lei n. 3.303, de 27 de junho de 2000: dispõe sobre normas de operação e uso da Internet no Brasil.

Projeto de Lei n. 3.016, de 16 de maio de 2000: dispõe sobre o registro de transações de acesso a redes de computadores destinados ao uso público, inclusive a Internet.

Projeto de Lei n. 76, de 27 de março de 2000: define e tipifica os delitos informáticos, e dá outras providências.

Projeto de Lei n. 1.589, de setembro de 1999: dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital, e dá outras providências.

Projeto de Lei n. 84, de 24 de fevereiro de 1999: dispõe sobre os crimes cometidos na área

inclusive convertidos em leis que estão em vigor, dentre os quais podemos destacar: o Decreto n. 3.505, de junho de 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal e recentemente o Projeto de Lei da Câmara dos Deputados n. 2957, de março 2008, ao qual estão apensados diversos projetos anteriores, todos relacionados à garantia da privacidade dos usuários e dados, da obrigatoriedade de o provedor realizar a adequada coleta e armazenamento de dados e da coibição ao envio de mensagens de correio eletrônicas indesejáveis.

Este tema deve ser estudado sempre com reflexão sobre os demais princípios do direito e normas vigentes sobre questões de privacidade, proteção patrimonial, sigilo profissional, direito à legítima defesa, bem como os direitos do consumidor, já que cabe às empresas proteger as bases de dados de seus clientes e ao Estado, com seu poder de polícia, proteger os usuários da Internet de um modo geral¹⁰⁸.

Todas estas ações e soluções, adequadas ou não, servem para que possamos extrair um caminho juridicamente viável e que possa atender, de certo modo, à proteção de um cidadão do mundo, seja ele virtual, seja real, uma vez que a maior característica da sociedade digital é encurtar cada vez mais a distância entre os ambientes reais e virtuais, em uma convergência que pode, um dia, significar a não distinção entre eles.

Para onde vamos com a Segurança da Informação? Ela tende a evoluir para ser mais holística, com uma abordagem mais comportamental, na qual não será apenas o uso de ferramentas que fará diferença na proteção, mas também a criação de uma cultura de proteção de conhecimento e reputação, afinal,

de informática, suas penalidades e dá outras providências.

Quanto à legislação em vigor, são elas:

Lei n. 9.983, de 14 de julho de 2000: altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 — Código Penal e dá outras providências.

Decreto n. 4.553, de 27 de dezembro de 2002: dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências.

Decreto n. 3.505, de 13 de junho de 2000: institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Projeto de Lei n. 7.131/2010, que dispõe sobre a responsabilidade dos proprietários e autores de *blogs* e mecanismos similares.

108. Devido a isso há a Convenção de Budapeste, que trata da colaboração internacional entre os países na investigação dos crimes eletrônicos, já que não há fronteiras físicas no mundo virtual (ver no capítulo crimes eletrônicos).

as informações, que são dados circulantes, representam justamente o patrimônio intangível de um indivíduo ou instituição. Por isso, a segurança deve estar nas pessoas e não apenas nos dispositivos e nos procedimentos.

8.13. Aspectos legais do monitoramento

Atualmente o monitoramento tornou-se um instrumento muito além da responsabilidade do empregador sobre o empregado¹⁰⁹, mais um fator de proteção de um ativo essencial para as empresas, a informação.

Conforme afirma Marcos Sêmola, em sua obra *Gestão da segurança da informação*: uma visão executiva, “o sangue da empresa é a informação. Distribuída por todos os processos de negócio, alimentando-os e circulando por diversos ativos”. De acordo com a referida citação, fica mais factível conceder à informação seu devido valor.

Dessa forma, podemos compreender melhor a afirmação feita no primeiro parágrafo, ou seja, o monitoramento não só garante ao empregador que estão sendo utilizados de forma correta os ativos disponíveis para realização do trabalho, mas atua resguardando a informação.

O assunto privacidade não é de fácil explanação e apresenta um nível de complexidade típico da sociedade atual, em que ao mesmo tempo que se valoriza o poder do indivíduo também se amplia o uso de escutas, câmeras, GPS, *softwares* de rastreamento etc.

A privacidade é um tema importantíssimo para a gestão legal da Segurança da Informação, com efeitos em diversas esferas. Em princípio, há alguns aspectos que precisam ser observados, sob pena de se cometerem infrações legais no gerenciamento e proteção dos ativos da empresa. Esses aspectos consistem em observar: a vida privada (assuntos de cunho pessoal), a interceptação (sigilo e confidencialidade tanto de pessoa física como jurídica), a prova obtida por meio ilegal ou legal e o anonimato.

Para tratar destes temas, vamos começar analisando a letra da lei. O art. 5º, X, da Constituição Federal de 1988 resguarda a intimidade e a privacidade, afirmando que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação.

109. Art. 932, III, do Código Civil: “São também responsáveis pela reparação civil: (...) III o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele”.

Privacidade, em tese, é a habilidade de uma pessoa controlar a exposição de sua vida pessoal, sua imagem, sua reputação, bem como a própria disponibilidade de informações acerca de si. Relaciona-se com a capacidade de existir na sociedade. No ordenamento brasileiro isso não representa o direito de ser anônimo que, ao contrário, está vedado pela Constituição Federal, no mesmo art. 5º.

A privacidade abrange, então, uma zona de intimidade, que significa a troca de expressões emocionais entre pessoas, do exercício de atividades intrínsecas ao indivíduo. Isso vai desde uma situação de estar nu, numa eventual ida ao banheiro, um assunto de separação judicial, e assim por diante.

O que ocorre é que, se não está claro que o ambiente não é privativo, então, ele se presume como tal. A não ser que se trate de espaço público e aberto, ou mídia de comunicação social, como é a Internet. Isso significa que não posso alegar infração a minha privacidade se estiver andando nu no meio da rua. Mas, por exemplo, o banheiro de dentro de uma empresa, em si, apesar de propriedade dela, traz consigo um princípio de privacidade, de zona de intimidade. Por isso a orientação legal é que seja feito sempre o aviso prévio no próprio ambiente quando este não for privativo ou estiver sujeito ao monitoramento.

O aviso serve para validar a captação de dados, imagens, sons. Para o uso deles posteriormente como prova, é fundamental que haja uma legitimidade da parte. Ou ela é o remetente ou o destinatário da mensagem, ou possuía uma autorização judicial para realizar a interceptação.

No caso da empresa, se ela deixa claro que o *e-mail* corporativo é de sua propriedade, que o ambiente é monitorado, inserindo essa informação nos rodapés de *e-mails* para dar publicidade inequívoca, possui uma política clara, então o uso de dados coletados nessa caixa postal corporativa não gerará problemas legais. Mas se tais etapas não forem cumpridas, não há presunção de propriedade da empresa; a presunção é de privacidade e vai favorecer a parte desprotegida, que na maioria dos casos é o funcionário.

A explicação está resumida, pois é importante realizar um estudo de cenários. Isso porque, se a mensagem é de caixa postal corporativa e está no servidor da empresa, a leitura dela neste ambiente não configura a interceptação. No entanto, se há uso de provedor de *e-mail* particular ou terceira empresa fornecedora, que passa a ser um intermediador da comunicação, então pode configurar interceptação.

O mesmo se a mensagem já foi baixada no HD do computador da empresa, na estação de trabalho, ou se ela se encontra em um equipamento pes-

soal, que não se restringe ao computador, pode ser um *notebook*, um *palm* ou outro dispositivo móvel, como um celular inteligente (*smartphone*) cada vez mais comum graças à popularização da tecnologia 3G.

E se for através de *MMS* ou *SMS*? É por isso que voltamos para a questão da definição clara de conceitos. O que é estação de trabalho? O que é de propriedade da empresa? O que é de particular? Tudo isso precisa ser bem esmiuçado para que a estratégia final gere a proteção legal adequada.

O fato de o anonimato não ser protegido no Brasil¹¹⁰ garante que por meio de medidas legais se possa sempre exigir a prestação de informações a respeito dos detentores da conta de *e-mail*, do IP, o remetente, o destinatário. Para isso, ressaltamos que é sempre bom adotar uma prática de formalizar essa solicitação, bem como sua resposta, para evitar que a empresa que presta esclarecimentos venha a ser imputada como infratora, seja da Constituição Federal, seja da Lei de Interceptação. Por esse motivo a resposta vem, em geral, apenas mediante ordem judicial¹¹¹.

O monitoramento de ambiente de navegação de Internet gera *logs* de histórico e eventos, fazendo com que seja possível traçar um perfil do que o

110. Art. 5º da Constituição Federal: “*Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) IV — é livre a manifestação do pensamento, sendo vedado o anonimato*”.

111. Em 2005 foi julgado no TST (Tribunal Superior do Trabalho) um recurso que envolvia monitoramento de *e-mail*, e a decisão foi a seguinte: “*Solução diversa impõe-se em se tratando do chamado ‘e-mail’ corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço*”. E continua: “*Se se cuida de ‘e-mail’ corporativo, declaradamente destinado somente para assuntos e matérias afetas ao serviço, o que está em jogo, antes de tudo, é o exercício do direito de propriedade do empregador sobre o computador capaz de acessar à INTERNET e sobre o próprio provedor. Insta ter presente também a responsabilidade do empregador, perante terceiros, pelos atos de seus empregados em serviço (Código Civil, art. 932, inc. III), bem como que está em xeque o direito à imagem do empregador, igualmente merecedor de tutela constitucional. Sobretudo, imperativo considerar que o empregado, ao receber uma caixa de ‘e-mail’ de seu empregador para uso corporativo, mediante ciência prévia de que nele somente podem transitar mensagens profissionais, não tem razoável expectativa de privacidade quanto a esta, como se vem entendendo no Direito Comparado (EUA e Reino Unido). Pode o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em ‘e-mail’ corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho. Inexistência de afronta ao art. 5º, incisos X, XII e LVI, da Constituição Federal*”.

usuário acessou. O que ocorre é que não está havendo interceptação de conteúdo, nem em princípio quebra de privacidade. Sendo corporativo, também não cabe a aplicação do Código de Defesa do Consumidor. Mas, dependendo de como é feito o relatório de monitoramento, e para qual finalidade ele é usado, se identifica indivíduos e *sites*, se é apenas para estatísticas gerais, pode gerar riscos civis, bem como trabalhistas.

Fora isso, aplicam-se as mesmas boas práticas para o monitoramento de *e-mail*. É importante ressaltar que, dependendo da ferramenta utilizada, se é por palavra-chave, se há uso de quarentena, se é chamado o funcionário para olhar junto ou não, se é dado o direito de explicação ou correção de conduta, se foi criada uma lista positiva (*White list*) e uma negativa (*Black list*), também há cuidados legais específicos a serem observados.

Os empregados cujo vínculo empregatício é regido pela CLT (Consolidação das Leis do Trabalho) e os empregados temporários podem ser advertidos do monitoramento pelo Contrato de Trabalho ou pela Política de Segurança. É interessante anexar a Política ao Contrato de Trabalho, pois dessa forma o empregado não poderá alegar desconhecimento da Política de Segurança.

Já para os demais colaboradores, que sejam prestadores de serviços que apresentam nota fiscal, pode haver a apresentação da Política de Segurança da Informação (PSI), caso exista, e se possível, um anexo ao contrato de prestação de serviços, ou a inserção da cláusula de monitoramento no próprio NDA ou Termo de Confidencialidade.

Quando se fala de confidencialidade é comum já existir uma cláusula no contrato ou um termo assinado entre as partes. No entanto, no tocante à segurança da informação há necessidade de cláusulas específicas, por isso, não é recomendável o uso das minutas muito antigas, que não trazem este tipo de redação mais atualizada¹¹². É importante fazer uma atualização dos

112. Modelo de cláusula de segurança da informação:

Cláusula XX — A CONTRATANTE poderá manter registros sobre todas as atividades relacionadas à execução do presente CONTRATO que sejam efetuadas através de acessos físicos ou lógicos às informações confidenciais, equipamentos, *softwares*, instalações, programas-fonte e quaisquer outros ativos de informação da CONTRATANTE, com o objetivo de:

a) apurar a observação da Norma de Segurança da Informação e do Código de Conduta aplicável ao terceirizado na execução dos serviços solicitados pela CONTRATANTE;

b) determinar ocorrência de algum comprometimento dos ativos de informação da CONTRATANTE, por exemplo, perda ou modificação de dados não autorizados;

contratos para evitar o uso de um texto que possa gerar mais riscos que prevenção.

Para os fornecedores e parceiros, os termos para contratação, conforme veremos mais adiante em Contratos (n. 11), estabelecerão a possibilidade ou não do monitoramento.

Quanto aos clientes, a situação é muito distinta das demais abarcadas. A melhor estratégia é o aviso formal, no rodapé do *site*, no rodapé dos *e-mails* eventualmente enviados pelo SAC, na política de privacidade *online*, na política de segurança da informação *online*, no termo de uso de serviços da Internet, ou nos próprios contratos¹¹³.

Em alguns casos específicos, principalmente se envolver mercado financeiro, por causa do princípio do sigilo bancário, faz-se necessário o aceite formal e específico dele para realização do monitoramento, o que deve ser feito nos *disclaimers* de dispositivos ou *softwares* de Internet *Banking* que são usados para prevenir fraude eletrônica e instalados no equipamento do usuário. Negligenciar tal atitude, ou seja, não avisar e requerer a autorização além da violação da privacidade, gera indenização civil. Pode-se incorrer no crime de interceptação de dados eletrônicos, previsto na lei de Interceptação.

c) identificar a divulgação e reprodução não autorizada de informações confidenciais;

d) auditar, por si ou por terceiro contratado, as responsabilidades contratuais e extracontratuais.

113. Exemplo de aviso de rodapé de *e-mail* corporativo *e-mail* de SAC:

Aviso Legal

Esta mensagem pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não deve usar, copiar ou divulgar as informações nela contida ou tomar qualquer ação baseada nessas informações. Este ambiente está sujeito a monitoramento.

Confidencialidade e Monitoramento:

Esta mensagem e quaisquer arquivos em anexo podem conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, por favor, não leia, copie, repasse, imprima, guarde, nem tome qualquer ação baseada nessas informações. Notifique o remetente imediatamente por *e-mail* e apague a mensagem permanentemente. Este ambiente está sendo monitorado para evitar o uso indevido de nossos sistemas. Outras informações sobre segurança e privacidade estão disponíveis em www.empresa.com.br.

Privacidade (especialmente para *e-mail* de marketing e SAC):

Esta mensagem e quaisquer arquivos em anexo podem conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, por favor, não leia, copie, repasse, imprima, guarde, nem tome qualquer ação baseada nessas informações. Notifique o remetente imediatamente por *e-mail* e apague a mensagem permanentemente. Aviso: não enviamos mensagens sem que tenha havido solicitação por parte do recipiente, nem solicitamos dados de cartão de crédito, senhas e outras informações pessoais por *e-mail*. Para saber mais sobre nossa Política de Privacidade, visite www.empresa.com.br

A boa prática consiste em aplicar uma estratégia de “*videogame*”, com uso de lógica indutiva, para programar a lei na interface, ou melhor, como já dissemos antes, “passar a regra do jogo, no próprio jogo”.

Como recomendações sobre as questões mandatórias do monitoramento, destacamos os seguintes pontos a serem observados pelas organizações: a) constar na Política de Segurança da Informação que o *e-mail* corporativo é monitorado; b) uma Norma de Uso de *E-mail*, deixando bem claro o que deve ou não ser feito com essa ferramenta; o empregado não pode ter expectativa de privacidade, ou seja, precisa estar informado de que o ambiente é não privativo (o que não é o mesmo que abrir mão da privacidade, que seria ilegal, por ser um direito *erga omnes*); e c) todos os empregados, bem como colaboradores, fornecedores, parceiros, que usarem ambientes monitorados devem ter ciência clara e inequívoca disso, se possível com aviso na própria via de comunicação (se telefone, a gravação prévia; se filmagem, o aviso na parede; se *e-mail* no rodapé; se na rede, no momento de autenticação nela, se na Internet, no momento de acesso a ela, como mensagem de sistema etc.).

Idealmente, deveria ser um fato de conhecimento geral que a caixa postal corporativa é de propriedade da Instituição, bem como os computadores e demais dispositivos que esta dispõe para seus funcionários (como exemplo: *pen drive*, CD-ROM, *notebook*, celular, acesso de internet etc.); o uso particular dessas ferramentas é o que motiva a polêmica atual. E é por isso que esse cenário precisa ser levado em consideração: para que o monitoramento ocorra como medida de prevenção e não de geração de risco jurídico.

Sendo assim, o monitoramento hoje vai além de uma medida de Segurança da Informação, pois o empregador é responsável pelos atos praticados por seus funcionários. É o que determina o art. 932¹¹⁴, III, do Código Civil¹¹⁵.

De acordo com a Súmula 341 do Supremo Tribunal Federal, a responsabilidade do patrão ou comitente pelos atos culposos de seus empregados¹¹⁶ ou prepostos é presumida.

114. “Art. 932. São também responsáveis pela reparação civil: (...) III — o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele.”

115. Ainda o referido diploma legal reza em seu art. 1.016:

“Os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções”.

116. Importante ressaltar a distinção existente entre empregado e preposto, qual seja, empregado é a pessoa que executa um serviço, trabalho ou função, sob as ordens de outra pessoa, de sua família, ou ainda relativa aos cuidados interiores do lar; preposto é aquele que está sob a

Como se não bastasse à referida súmula, o Código Civil em seu art. 933¹¹⁷ determina que a responsabilidade do empregador é objetiva, isto é, independe de culpa.

Dessa forma, como já foi elucidado, a monitoração é um instrumento bastante útil para gerenciar o risco legal e ainda colabora na gestão da Segurança da Informação. Entretanto, nossa Constituição Federal, em seu art. 5º, X, assegura o Direito a Privacidade e a Intimidade, o que, em princípio, poderia gerar uma interpretação de que haveria conflito com a atividade de monitoramento.

Para evitar infração à Lei Maior, é essencial que o monitoramento corporativo ocorra com prévio aviso e ciência dos funcionários, inclusive com publicação de norma própria e inserção desse aviso nos ambientes eletrônicos (especialmente o de *login* na rede e o rodapé de *e-mail*).

No entanto, apesar do aviso, a “câmera” não escolhe o que está gravando. Por isso, pode ocorrer que o monitoramento acabe gerando acesso a conteúdos de ordem particular, íntima e pessoal que estejam trafegando no *e-mail* corporativo ou que tenham sido salvos ou armazenados nos computadores ou servidores da empresa.

Por esse motivo o monitoramento deve ser realizado por uma equipe treinada, e ocorrer de modo centralizado, com procedimentos-padrão, nas quais o relatório de monitoramento deve ser utilizado apenas para fins de investigação de casos específicos, em que se demonstre infração ao código de conduta, prática de ilícito ou crime, ou mediante solicitação das Autoridades Competentes.

O momento é bastante oportuno para destacar a célebre decisão do Tribunal Superior do Trabalho sobre a validade de prova obtida por meio do monitoramento de *e-mail* corporativo, mais especificamente o Processo n. 613-2000-013-10-00, onde o Ministro João Oreste Dalazen assegura que:

“...pode o empregador monitorar e rastrear a atividade do empregado no ambiente de trabalho, em *e-mail* corporativo, isto é, checar suas mensagens, tanto do ponto de vista formal quanto sob o ângulo material ou de conteúdo. Não é ilícita a

vinculação de um contrato de preposição, isto é, um contrato em virtude do qual certas pessoas exercem, sob a autoridade de outrem, determinadas funções subordinadas, no seu interesse e sob suas instruções, e que têm o dever de fiscalizá-las e vigiá-las, para que proceda com a devida segurança, de modo a não causar dano a terceiros.

117. “Art. 933. As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos.”

prova assim obtida, visando a demonstrar justa causa para a despedida decorrente do envio de material pornográfico a colega de trabalho".

Ainda dentro dessa seara o Ministro salienta que tal monitoração deve ser feita "*de forma moderada, generalizada e impessoal...*", e continua justificando porque a empresa pode rastrear e monitorar: "*...porque não haveria qualquer intimidade a ser preservada, posto que o e-mail não poderia ser utilizado para fins particulares...*".

Para finalizar sua decisão, o Ministro Dalazen enfatizou que os direitos do cidadão a privacidade e sigilo de correspondência, constitucionalmente assegurados, restringem-se à comunicação pessoal. Já o *e-mail* corporativo é cedido ao empregado pelo empregador, de forma, que, sendo propriedade do empregador, é permitido a este (empregador) exercer controle tanto formal como material (conteúdo) das mensagens que trafegam pelo seu sistema de informática.

Outro fundamento utilizado foi a Lei inglesa RIP — *Regulation of Investigatory Power* —, na qual o empregador tem poderes para rastrear e monitorar não só *e-mail* como telefonemas de seus empregados.

É importante destacar que o monitoramento de ambientes em que não haja aviso claro, isto é, sem a devida ciência do usuário e sem esclarecimento por parte do empregador quanto à propriedade dos recursos informacionais, pode configurar crime da Lei n. 9.296/96 (interceptação), que estatui:

"Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa".

Deve-se frisar, também, que a atribuição da responsabilidade do empregador é presumida desde que o empregado ou preposto esteja agindo dentro dos limites da sua função. Por isso recomendamos que o empregador utilize os Termos de Responsabilidade para estabelecer quais são as funções dos profissionais das áreas de Segurança de Informação que deverão executar as atividades de análise de relatórios de monitoramento.

Acrescenta-se, por oportuno, que o monitoramento pode ser feito de diversas maneiras. A forma mais comum é o uso de *software*, que permite separar, por meio de filtros, "palavras-chave", conteúdos de *e-mail* para análise, bem como permite verificar os endereços de Internet que sejam acessados a partir da rede da empresa. Logo, não há, inicialmente, por parte do *software*, um juízo de valor sobre o conteúdo monitorado. Tal avaliação é feita por uma

pessoa encarregada para tanto, que deve apresentar o diagnóstico à Diretoria, que, por sua vez, irá tomar as medidas cabíveis, quando for o caso.

É fundamental que o acesso às informações geradas pela monitoração seja restrito, e seu uso limitado para fins de investigação ou análise de incidentes, para evitar que a divulgação interna indiscriminada, com identificação de usuários, conteúdos e condutas, venha a gerar um risco legal de dano moral por parte da empresa.

Sendo assim, o monitoramento, quando bem empregado, com uso de procedimentos adequados, permite pegar o infrator e proteger o inocente. Já seu uso sem as devidas cautelas pode gerar risco legal.

Como dito, já existem diversos casos na Justiça brasileira em que o conteúdo de *e-mail* monitorado foi utilizado como prova para demissão de um funcionário por justa causa, no caso de flagrante violação de sigilo profissional¹¹⁸.

Com relação ao funcionalismo público, a tendência tem sido a mesma. No Brasil, temos a decisão do Supremo Tribunal Federal em caso similar, em que funcionário do Tribunal de Contas da União (TCU) violou a Política da referida Instituição e, dessa forma, foi punido com a retirada do acesso¹¹⁹.

118. Em 1999 um funcionário foi demitido por justa causa de empresa desenvolvedora de *software*. O empregado repassava para outra empresa os *softwares* que estavam sendo desenvolvidos naquela (empregadora). No Acórdão, n. 19990455727, destaca-se ementa do Relator: "*FALTA GRAVE — A fídicia é o elo que liga patrão e empregado e, como uma planta frágil, há de ser regada diariamente para que cada vez mais se acentue e se fortaleça. Neste caso, a fídicia restou em frangalhos quando a empresa constatou que o autor, na qualidade de empregado de confiança, desenvolvia 'software' para uso desta e o passava para outra empresa*".

119. ACÓRDÃO DO SUPREMO TRIBUNAL FEDERAL: MANDADO DE SEGURANÇA

(Tribunal Pleno)

MS-AgRg 23.514 / DF — DISTRITO FEDERAL

AG. REG. NO MANDADO DE SEGURANÇA

Relator(a): Min. MAURÍCIO CORRÊA

Julgamento: 3-11-1999 — Órgão Julgador: Tribunal Pleno

Publicação: DJ, 17-3-2000, p. 00020 EMENT. VOL-01983-02 PP-00259

Parte(s)

Agte.: Ricardo Luiz Rocha Cubas

Agdo.: Presidente do Tribunal de Contas da União

EMENTA: AGRAVO REGIMENTAL EM MANDADO DE SEGURANÇA. NÃO CABIMENTO DA AÇÃO MANDAMENTAL: INEXISTÊNCIA DE LEI QUE ASSEGURE AO IMPETRANTE O DIREITO PLEITEADO NO *WRIT*. FATOS CONTROLADOS. FACULDADE CONFERIDA AO RELATOR PELO ARTIGO 21, § 1º, DO

A monitoração, além de instrumento hábil de exclusão da responsabilidade ou de detecção de usuário e posterior direito de regresso, é crucial para aprimoramento e garantia da Segurança da Informação da empresa. Para garantir à empresa o acesso às suas próprias informações, em suas próprias caixas de correio eletrônico, HD's de computadores, arquivos de rede, é essencial que haja aviso prévio do monitoramento, que deve constar em norma expressa da empresa.

No entanto, a execução prática do monitoramento exige a elaboração de um procedimento-padrão que evite riscos legais, com acesso restrito aos conteúdos objeto dele e muita cautela no uso destes, sempre motivado e dentro de um limite de proporcionalidade. Isso para evitar situações que não tenham qualquer natureza de monitoramento, mas sim de uma divulgação vexatória e mal intencionada de aspectos relacionados à vida pessoal, da geração de estatísticas de produtividade abusivas ou da motivação injustificada de uma demissão¹²⁰.

Ou seja, muitas vezes a informação coletada e não o monitoramento em si é que pode gerar o risco legal. Por isso, o treinamento dos funcionários da empresa é essencial, especialmente dos que se ocupam de cargos de chefia.

RISTF. INTERVENÇÃO DO MINISTÉRIO PÚBLICO: DESNECESSIDADE. 1. Convencido o Relator do não cabimento do *writ* pela falta de prova pré-constituída, pela inexistência de lei que gere direito líquido e certo ao impetrante, e por apoiar-se a impetração em fatos controvertidos, aplicável é o artigo 21, § 1º, do RISTF. 2. Não é obrigatória a intervenção do Ministério Público se o mandado de segurança é indeferido de plano. Agravo regimental não provido.

6. Ademais, inexistente regra jurídica que assegure ao agravante o uso do "e-mail" para interesses particulares ou que impeça sua exclusão do rol dos usuários por desobediência às normas estabelecidas pelo TCU, sendo impertinentes as alegações de que os princípios constitucionais da isonomia, do devido processo legal, do contraditório e da ampla defesa teriam sido violados, visto que cabe à Administração dispor sobre a utilização dos instrumentos oferecidos a seus servidores, ampliando ou restringindo o alcance de cada um deles, de acordo com sua conveniência.

120. Número do processo: 00921-2001-291-04-00-8 (RO)

Juiz: FLAVIO PORTINHO SIRANGELO

Data de Publicação: 6-3-2006

EMENTA: Dano moral. Quando se caracteriza. Indenização devida. Divulgação da despedida através de e-mail dirigido a um grupo expressivo de quase 80 empregados ou colaboradores da reclamada, realizada por representante legal da empresa, dando notícia da demissão do autor por justa causa e que contém inequívoca divulgação do pretense ato de improbidade que lhe foi injustamente imputado. Ainda que se entenda que o ato da demissão por justa causa, em si mesmo, não é capaz de caracterizar o dano moral, a sua publicidade, através da divulgação unilateral dos fatos à coletividade de pessoas na qual esteve integrado o reclamante por mais de 20 anos, permite concluir que tal divulgação contribuiu para afetar negativamente o conceito do reclamante, dando causa, neste caso, ao sofrimento gerador de dano moral que reclama reparação, na forma de direito. Aplicação de precedentes da jurisprudência dos tribunais em casos análogos. Recurso do autor provido neste item.

8.14. Aspectos legais do BYOD e a mudança da CLT

Quais os impactos da mobilidade nas relações de trabalho? Estamos trabalhando 24 horas diárias sem desligar? Esta é uma questão delicada que deve ser enfrentada, e iniciamos 2012 com essa discussão devido à alteração do art. 6º da Consolidação das Leis do Trabalho — CLT. O que as empresas podem fazer para minimizar os riscos?

O objetivo da alteração na CLT foi o de equiparar o empregado que está presencialmente na empresa com o empregado que trabalha remoto, no modelo de "Home Office" ou teletrabalho. Ou seja, a nova Lei n. 12.551, de dezembro de 2011, apenas formalizou um entendimento que já havia no judiciário, de ser indiferente o local em que o funcionário está fisicamente para que ele tenha os mesmos direitos previstos na legislação trabalhista.

No entanto, com a redação dada a seu parágrafo único, abriu-se margem para uma interpretação de que o recebimento da mensagem já configuraria colocar o funcionário em trabalho, impactando o entendimento sobre hora extra e sobreaviso, isto é, quando o funcionário exerce uma atividade laboral após o horário normal do seu turno ou expediente.

Isso é apenas uma interpretação retirada do texto de lei, mas que pode impactar muito o modelo de trabalho da Sociedade Digital, uma vez que o entendimento tende a ser mais favorável aos interesses do empregado. Isso se deve porque a informação circula independentemente do horário, especialmente com o aumento da força de trabalho com a geração Y, em que o próprio empregado já possui recursos de mobilidade e os utiliza, ainda que a empresa não os tenha fornecido.

Em depoimento à imprensa, o presidente do TST, João Oreste Dalazen, afirmou que "a meu juízo, é inafastável a revisão da súmula em face da superveniência da lei, a lei passou a dizer que o trabalho realizado a distancia é tempo de serviço". Ele se refere à Súmula 428, de 24 de maio de 2011, pela qual o Tribunal assentou o entendimento de que "o uso de aparelho de intercomunicação, a exemplo de BIP, pager ou aparelho celular, pelo empregado, por si só, não caracteriza o regime de sobreaviso". Afinal, não é pelo fato de ter acesso a informação, de meramente portar o recurso, que significa que a pessoa foi soliciitada a trabalhar.

Muito pelo contrário, as empresas têm sido obrigadas a bloquear o acesso do colaborador quando sai de férias, pois as pessoas estão cada vez mais "conectadas e ligadas" o tempo todo e não querem esperar o dia seguinte ou o

início do expediente para saber o que está acontecendo ou para tomar providências proativas de trabalho.

No cenário mais competitivo do mercado atual, sem fronteiras e de alcance global, a proatividade ocorre por liberalidade do próprio profissional, que busca mostrar serviço mesmo que a empresa não tenha solicitado.

Pela interpretação da Lei, três situações podem ocorrer quando um colaborador recebe uma mensagem relacionada a trabalho após o expediente, ao acessar seu *e-mail*, utilizar um *smartphone* ou dispositivo similar:

a) entender que essa hora de serviço à disposição da empresa deve ser paga como sobreaviso (o trabalhador receberia pelo período, à equivalência de um terço do salário);

b) considerar o período como hora normal de trabalho, podendo ser caracterizada a hora extra;

c) a empresa não pagar nada pelo serviço à disposição, analisando essa questão sob a ótica do tipo de recurso (celular, *pager*, *e-mail*, telefone fixo, redes sociais, entre outros).

A nova Lei teve intenção de consolidar o trabalho remoto, mas acabou impactando, mesmo que não intencionalmente o “Mobile Office”, ou seja, o comportamento do trabalho na era da mobilidade, em que o profissional quer receber seus *e-mails* corporativos no *smartphone* e estar a par do que ocorre no âmbito profissional, mesmo que isso não tenha sido solicitado.

Se o mero recebimento de um *e-mail* for entendido como ordem direta, independentemente do conteúdo ou do que foi solicitado, muitas empresas vão acabar suspendendo ou bloqueando o acesso às informações fora do horário de expediente. Isso tornará o Brasil menos competitivo. Ou seja, querer antecipar a conversa, a informação, o que é recorrente no dia a dia atual vai virar um risco de hora extra e sobreaviso. Imagine isso em uma agência de publicidade, por exemplo.

Esse comando segue na contramão do que é preciso ajustar na legislação trabalhista, que precisa evoluir e permitir jornada flexível, regras definidas entre as partes, e que empregador e empregado possam combinar como será o trabalho sem receio de isso depois ser alterado no judiciário. Logo, é necessário que as partes, empregador e empregado, regulem isso. A falta de regra interna própria definida e o advento da nova lei certamente acarretarão um clima de insegurança sobre o regime de trabalho e o receio de condenação por pagamento de verbas adicionais, pois é praticamente impossível controlar a circulação da informação.

Como a Lei já entrou em vigor, cabem algumas recomendações urgentes para as empresas que querem evitar interpretações desfavoráveis e riscos trabalhistas maiores, visto que o cenário atual já é o de mobilidade corporativa:

- ✓ Rever a atribuição de função e cargo e a documentação de quais são os cargos de confiança alinhados com o previsto na legislação;
- ✓ Rever a concessão dos recursos corporativos que permitem comunicação e informação independentemente de horário de jornada de trabalho para profissionais que não sejam de cargo de confiança (especialmente *smartphone*, *notebook*, VPN e *tablets*), bem como o horário em que as pessoas podem ter acesso ao correio eletrônico corporativo (eventualmente implantar uma ferramenta de gestão diferenciando o perfil e o horário conforme a função);
- ✓ Elaborar a Norma de Uso de Recursos de Mobilidade deixando claros os dois cenários — quando for a empresa que fornece o recurso corporativo e quando for o colaborador que o possui, além de destacar que o fato do mero recebimento da informação não significa que ele foi solicitado a trabalhar. O fato de ter ou manusear o recurso não reflete que está automaticamente de sobreaviso ou que o pagamento de hora extra será devido *incontinenti*, implicando uma análise caso a caso;
- ✓ Não é porque o *e-mail* chegou ao aparelho de telefone, ou um torpedo, que o colaborador estava esperando por isso, com restrições até de sua vida pessoal e da sua livre circulação. Lembramos que o sobreaviso exige inclusive que haja um dever de responder e um tempo máximo de espera, muitas vezes com restrição de perímetro físico que o funcionário pode estar;
- ✓ Treinamento para chefes e gestores sobre como compartilhar informações, seja por *e-mail*, torpedo, comunicador instantâneo e até *post* em redes sociais sem que o texto represente solicitação de serviço, para que fique claro que é uma liberalidade do colaborador querer tomar conhecimento da informação compartilhada;
- ✓ Mapear e levantar as situações que de fato o colaborador deve assumir providências a partir do recebimento de mensagens fora do horário de expediente e, se for o caso, rever o horário da jornada de trabalho para adequação do novo cenário (especialmente empresa que tem presença em outros países e há comunicação em fuso horário distinto);
- ✓ Ter conhecimento das equipes que atendem e postam conteúdo em redes sociais, que muitas vezes podem não depender de uma jornada

de trabalho fixa para ocorrer, pois os reflexos são instantâneos e com demanda de resposta imediata. Dependendo da situação, pode-se decidir terceirizar a atividade para evitar maiores riscos trabalhistas, pois nessa hipótese se admite haver a incidência de ambos adicionais, aumentando em média em 1/3 o custo com aquele funcionário.

- ✓ Além disso, devemos considerar ainda o cenário do BYOD, cuja sigla significa em inglês *Bring Your Own Device*, no qual não é mais a empresa que fornece o recurso corporativo tecnológico, mas sim o profissional que traz e usa o seu recurso particular no ambiente de trabalho. Esta situação híbrida provoca vários impactos jurídicos e alguns riscos relacionados à privacidade e à segurança da informação, que merecem tratamento especial.

Sendo assim, como a empresa deve agir com o uso cada vez maior de dispositivos pessoais no ambiente de trabalho? Do ponto de vista jurídico, é melhor assumir o modelo, proibir ou fazer vista grossa?

Com a consumerização, aumenta a análise de viabilidade de implementação de uma Política de BYOD no ambiente corporativo, inclusive em instituições de ensino. Afinal, muitos profissionais preferem usar seu próprio equipamento, que em geral é até melhor do que o oferecido pela empresa.

O primeiro passo é estabelecer as regras claras. Deve ficar muito bem definido de quem é a propriedade do equipamento, quais os requisitos de segurança que deverá cumprir, bem como quais as obrigações e limites de seu uso. Há uma grande diferença em termos de gestão da TI, quando a empresa deixa de ser quem fornece o recurso e passa a ser beneficiária do uso do recurso particular de seu colaborador ou de um terceiro. Além disso, apesar do benefício da economia de gastos com equipamentos, há sim uma perda relativa de controle de qual tipo de conteúdo ou *softwares* estarão no dispositivo.

É importante ressaltar que cabem ao proprietário do equipamento todos os deveres no tocante à manutenção e guarda do mesmo, bem como a responsabilidade por todo e qualquer conteúdo armazenado. No entanto, quando se trata de *softwares* para uso em benefício da empresa, há um grande risco de ela ser envolvida em um incidente de pirataria, caso o equipamento faça uso, por exemplo, de um editor de texto e planilhas sem a devida licença respectiva, pois, aí, o resultado do trabalho foi gerado a partir de um *software* pirata com o conhecimento da empresa, o que gera implicações legais.

Por conta disso, muitas empresas tratam do cenário de forma híbrida, em que o equipamento é do usuário, mas a camada de *softwares* é fornecida pela

empresa, de modo a tentar mitigar riscos com pirataria. Outro ponto a observar envolve a questão trabalhista, devido à alteração do art. 6º da CLT. Por isso, a política deve prever que o acesso ao recurso, por si só, não configura sobreaviso nem sobrejornada.

Sendo assim, para evitar riscos, cabe à empresa deixar claro na política de BYOD que:

- ✓ o equipamento é de completa responsabilidade do proprietário;
- ✓ o conteúdo armazenado é de responsabilidade do proprietário;
- ✓ o proprietário declara que todos os *softwares* possuem licença regular sob pena de responder isoladamente sobre qualquer incidente de pirataria;
- ✓ o proprietário deverá fazer uso de requisitos mínimos de segurança da informação, mas não se limitando a antivírus, *antispyware*, senha de bloqueio, criptografia;
- ✓ o proprietário tem o dever de realizar *backup* de todas as informações pertinentes à empresa e de salvá-las na rede corporativa;
- ✓ o equipamento está sujeito a monitoramento e a inspeção física por parte da empresa;
- ✓ o equipamento está sendo colocado à disposição da empresa como beneficiária de uso temporário e parcial, em caráter não oneroso, sem qualquer responsabilidade por parte da empresa;
- ✓ a empresa não se responsabiliza por perda, deterioração, furto, extravio, quebra do equipamento e, se isso vier a ocorrer, o proprietário deverá avisar à empresa imediatamente;
- ✓ o proprietário compromete-se a portar o equipamento de forma discreta e com o máximo de zelo possível, para evitar incidentes e vazamentos de informação da empresa;
- ✓ o mero acesso ou uso do equipamento ou recursos de informação pelo proprietário, por si só, não configura sobreaviso ou sobrejornada, sendo um ato de liberalidade, proatividade e iniciativa do mesmo.

Para concluir, é fundamental não confundir os limites entre ser o proprietário do equipamento (que no caso passa a ser o indivíduo) e ser o beneficiário (que passa a ser a empresa). Se a empresa oferecer realizar manutenções, trocar peças, consertar o aparelho, ou seja, realizar todas as atividades intrínsecas à responsabilidade de proprietário, acabará atraindo para si todo o ônus de zelo do bem, gerando riscos legais em sua política de BYOD.

8.15. Documentos eletrônicos

Uma característica própria da sociedade digital é a crescente tendência de diminuição do uso de documentos físicos na realização de contratos, propostas e mesmo para a divulgação de obras, produtos e serviços, implicando a modificação de uma característica básica que se tornou comum em nosso modelo de obrigações: o uso do papel.

Mas o papel, em última análise, é nada mais que uma tecnologia também, que passou a permitir, como um tipo de suporte físico, que a manifestação de vontade ficasse mais claramente evidenciada entre as partes de uma relação.

A problemática da substituição do papel, no entanto, é mais cultural que jurídica, uma vez que nosso Código Civil prevê contratos orais¹²¹ e determina que a manifestação de vontade pode ser expressa por qualquer meio¹²². Quem disse que porque está no papel é o documento original? Afinal, todo fax é cópia, apesar de estar em papel. Já o *e-mail* eletrônico é o original, e sua versão impressa também é cópia.

Logo, na verdade, percebemos que o ser humano é um ser material por natureza, tendo apenas a espiritualidade como elemento imaterial. Todo o resto necessita de representação física para se poder ter o sentimento de posse, de propriedade. Esse sentimento não será resolvido nem mudado pelo Direito tradicional nem pelo Direito Digital. O que se tem de fazer é encontrar caminhos em que a tecnologia possibilite dar esta impressão de materialidade aos documentos eletrônicos.

Ocorre que, para haver esse desapareço ao papel¹²³, é preciso criar uma nova metodologia para a certificação de documentos e de assinaturas com formato digital, ou seja, não físico, no sentido material. Emocionalmente nos sentimos mais protegidos quando há um documento por escrito, uma prova material, palpável, de nossos direitos. Por isso, já há normas tratando da matéria, que teve

121. Como exemplo podemos citar o *caput* do art. 656 do Código Civil, referente ao mandato: “Art. 656. O mandato pode ser expresso ou tácito, verbal ou escrito”.

122. Art. 107 do Código Civil: “Art. 107. A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir”.

123. A Receita Federal editou no dia 13 de março de 2006 a Portaria n. 259, que acaba com o uso do papel nos processos para os contribuintes que possuírem certificação digital. Os documentos vão passar a ser apresentados eletronicamente. A novidade foi anunciada pelo secretário-adjunto da Receita Federal, Paulo Ricardo de Souza Cardoso. Com a edição da medida, os contribuintes com certificado digital poderão entregar documentos, peticionar, apresentar pedidos, recibos, tudo de forma eletrônica.

início com a questão da emissão de CPF e CNPJ pela Internet por órgão da Receita Federal¹²⁴. Devemos lembrar que países como Argentina¹²⁵ e Uruguai¹²⁶ já regulamentam o documento eletrônico, o que os coloca em vantagem competitiva para a realização de negócios.

No Brasil destacamos ainda a questão da digitalização registrada, que corresponde ao processo de transladação do documento original do suporte em papel para digital e seu registro para guarda permanente e consulta, preservados como originais, com o mesmo valor jurídico do original, não como cópia autenticada, digitalizada ou microfilmada. O registro é efetuado em Cartório de Registro de Títulos e Documentos, seguindo os ditames da Lei Federal n. 6.015/73, que dispõe sobre os registros públicos e dá outras providências¹²⁷.

A questão sobre documentos eletrônicos não é criação da Internet. É um assunto que já se discute há muito tempo¹²⁸ devido à documentação de operações em redes eletrônicas de bancos, seja via intranet de computadores ligados com operadoras de cartão de crédito, seja quanto a aplicações financeiras rea-

124. Ver Instrução Normativa SRF n. 462, de 19 de outubro de 2004, que institui o Serviço Interativo de Atendimento Virtual, e aprova os leiautes de referência dos cartões inteligentes (*smart cards*) para armazenamento de certificados digitais e-CPF e e-CNPJ, e a Instrução Normativa n. 580, de 12 de dezembro de 2005, que institui o Centro Virtual de Atendimento ao Contribuinte da Secretaria da Receita Federal (e-CAC). Segundo o presidente da Câmara Brasileira de Comércio Eletrônico e membro do Comitê Gestor da ICP-Brasil, Manuel Matos, nos próximos dois anos, por pressão da Receita Federal e atuação dos principais bancos do País, o número de usuários de e-CPFs e e-CNPJs deverá saltar dos atuais 500 mil para mais de 5 milhões, podendo chegar aos 20 milhões até o final da década.

125. Com o Decreto n. 427, de 16 de abril de 1998, a Argentina regulamentou a assinatura digital apenas no âmbito da Administração Pública.

126. O Uruguai, através da promulgação da Lei n. 16.002, de 25 de novembro de 1988, posteriormente alterada pela Lei n. 16.736, de 5 de janeiro de 1996, universalizou a origem e o destino do documento eletrônico, para fins de reconhecimento legal.

127. A Lei Federal n. 6.015, de 31 de dezembro de 1973, traça o arcabouço normativo registral para que seja conferida a autenticidade, segurança e eficácia dos atos jurídicos, sejam eles efetivados por documentos públicos ou particulares. Já a Lei Federal n. 8.935, de 18 de novembro de 1994, seguindo a linha do diploma registral, define os serviços notariais e de registro como os de organização técnica e administrativa destinados a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos.

128. Vide a Lei de Microfilmagem — Lei 5.433/68 — Art. 1º “É autorizada, em todo o território nacional, a microfilmagem de documentos particulares e oficiais arquivados, estes de órgãos federais, estaduais e municipais.

§ 1º Os microfilmes de que trata esta Lei, assim como as certidões, os traslados e as cópias fotográficas obtidas diretamente dos filmes produzirão os mesmos efeitos legais dos documentos originais em juízo ou fora dele”.

lizadas remotamente na Bolsa de Valores¹²⁹, seja via telefone em operações conduzidas pelo cliente em uma gravação eletrônica, nos serviços de *bank phone*¹³⁰.

É ilusão acreditar que o papel é o meio mais seguro. O papel em si não confere garantia de autenticidade e integridade, tampouco amarra a assinatura das partes com o conteúdo. Para receber esta característica de prova plena¹³¹, precisa seguir os requisitos determinados na Lei de Registros¹³². Por sua vez, os Cartórios passaram a guardar a documentação também digital.

Do exposto, verificamos que devemos tratar o tema da documentação eletrônica em três níveis: a) Cultural (quebra de usos e costumes visto que papel e originalidade não têm equivalência); b) Técnico (já que há necessidade de definição do melhor procedimento para tratar a documentação digital ou digitalizada, como já foi feito em 1968 e 1996 na questão do microfilme; e c) Jurídico (pois é preciso que a técnica permita preservar capacidade de prova de autoria e integridade, que seja auditável e periciável, que tenha segurança da informação, que tenha, quando preciso, fé pública (visto que o documento físico quando já nascido com falsidade, não é nem o fato de estar no papel, nem sua autenticação no cartório que vão lhe conferir validade jurídica).

129. Ver Deliberação CVM n. 365, que estabelece a obrigatoriedade de auditoria de sistemas nas corretoras de valores mobiliários que utilizam o sistema de negociação via Internet mantido pela Bolsa de Valores de São Paulo, bem como o Parecer Orientativo CVM n. 32, que tem por objetivo explicitar o entendimento da Comissão de Valores Mobiliários quanto à caracterização (i) de uma oferta de distribuição de valores mobiliários como pública, quando a Internet é utilizada como meio de comunicação, com base na interpretação do art. 19, § 3º, III, da Lei n. 6.385/76, e (ii) de exercício de atividade sujeita à autorização da Comissão de Valores Mobiliários, quando a atividade é exercida por intermédio da Internet, nos termos do art. 16 da mesma lei. E o Parecer Orientativo CVM n. 33.

130. A Resolução CVM n. 2.817 dispõe sobre a abertura e a movimentação de contas de depósitos exclusivamente por meio eletrônico, bem como acerca da utilização desse instrumento de comunicação.

131. É pela fé pública, pois, que os documentos particulares, sejam em papel ou em meio digital, adquirem a eficácia da prova plena, conforme disciplina o art. 217 do Código Civil, bem como o art. 161 da Lei n. 6.015/73.

132. O art. 127, I, da Lei n. 6.015/73 dispõe que é da competência do registro de títulos e documentos o registro *“dos instrumentos particulares, para a prova das obrigações convencionais de qualquer valor”*; Por características próprias dos atos registrais e, especificamente no caso do registro de títulos e documentos, suas certidões produzem o mesmo valor probante que o original, conforme dispõe o art. 161 da Lei n. 6.015/73, somente sofrendo impugnação que tenha como objeto de discussão a validade ou autenticidade do próprio documento original. Já os arts. 6º e 7º da Lei n. 8.935/94 disciplinam as atribuições dos notários e registradores que serão competentes para intervir nos atos e negócios jurídicos sobre os quais as partes devam ou queiram atribuir a forma legal ou autenticar fatos e cópias, e reconhecendo firmas, e ao registrador os atos pertinentes à legislação dos registros públicos.

Logo, sabemos que armazenar dados e imagens em discos rígidos ou fitas é muito mais seguro que arquivá-los em papel, desde que o processo seja feito de modo adequado. É uma obrigação de todos os operadores digitais esclarecer, explicar e ensinar como adequadamente registrar operações eletrônicas e cabe ao Estado determinar qual será o padrão de conduta para a certificação¹³³ dos documentos, considerando que a tecnologia permite que isso seja feito automaticamente, sem a burocracia dos cartórios do mundo real¹³⁴, com o diferencial de ainda poder ser auditado. Recomendamos a leitura do item 8.49, sobre Gestão Eletrônica de Documentos.

8.16. Prova eletrônica

Não há nenhuma legislação brasileira que proíba ou vete a utilização de prova eletrônica¹³⁵. Ao contrário, o Código Civil e o Código de Processo Civil aceitam completamente o seu uso, desde que sejam atendidos alguns padrões técnicos de coleta e guarda, para evitar que esta tenha sua integridade questionada ou que tenha sido obtida por meio ilícito¹³⁶. Logo, o que realmente exis-

133. O Poder Executivo, por meio da Medida Provisória n. 2.200, que teve sua primeira edição em 28 de junho de 2001, sendo revista em 24 de agosto do mesmo ano, institui a Infraestrutura de Chaves Públicas no Brasil e começou a regulamentar a assinatura digital. Em seguida veio o Decreto n. 3.872, de 18 de julho de 2001, que dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (CGICP-Brasil).

134. Ocorre ultimamente um debate sobre a certificação digital. Acreditam alguns que, por força do art. 236 da Constituição Federal, os tabeliães de notas teriam o monopólio do certificado digital. Discordamos, porém, dessa linha de pensamento. Acreditamos que a certificação da assinatura digital pode ser feita por qualquer particular, como de fato já vem sendo feita por grandes empresas privadas, para que o processo certificatório seja o mais célere, menos burocrático e consequentemente menos oneroso.

135. Art. 225 do Código Civil: *“As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão”*.

136. Nas palavras do Dr. Alexandre Guimarães Gavião Pinto, Juiz de Direito do TJRJ: *“De acordo com o artigo 5º, inciso LVI da Constituição da República são inadmissíveis, no processo, as provas obtidas por meios ilícitos, o que importa no reconhecimento de que todo meio de colheita de prova que vulnere as normas do direito material deve ser combatido, o que configura, indubitavelmente, importante garantia em relação a ação persecutória do Estado. A prova ilícita nada mais é do que uma espécie da denominada prova proibida, que deve ser entendida como toda aquela que não pode ser valorada no processo. Não se pode perder de perspectiva a existência de duas espécies de provas proibidas, que são: as provas ilícitas e as provas ilegítimas. As provas ilícitas são aquelas alcançadas com a violação do direito material, enquanto as provas ilegítimas são as obtidas em desrespeito ao direito processual. A prova ilícita não pode ser considerada idônea para formar o convencimento do Magistrado, devendo ser desprezada, ainda que em prejuízo da apuração da verdade, o que se justifica diante da necessidade de*

te, novamente, é o preconceito quanto ao tipo de prova, pois todos nós temos medo (insegurança) daquilo que não conhecemos.

Já vimos que a documentação em papel está em fase de transição, passando a ser eletrônica, relevante para a produção de provas em Direito. Aos poucos, evoluímos de um suporte limitado, com baixa tecnologia de segurança, para um ambiente independente de suporte, em que é possível replicar originais eletrônicos e de valor original e não de cópia. É de se saber que tudo em meio eletrônico deixa rastro.

Os operadores do Direito devem saber o que é um documento original eletrônico, principalmente aqueles que são da geração Y. Por isso devemos ser multidisciplinares, estrategistas, inovadores com pensamento transversal e compreender a tecnologia.

A evidência digital é toda informação ou assunto de criação, intervenção humana ou não, que pode ser extraído de um compilado ou depositário eletrônico. E essa evidência deve estar em um formato de entendimento humano. Caso contrário, poderá ser considerada um artefato, que explicaremos de forma mais precisa no item 8.16 deste livro (prova eletrônica).

Para se ter informações básicas e necessárias para coleta e guarda para os provedores de acesso, é necessário ter o registro de logs e os registros cadastrais dos usuários de IPs (fixos e dinâmicos). Os provedores de e-mails, por sua vez, devem verificar os registros de conexão e registros cadastrais dos usuários dos

se formar um processo justo, que respeite os direitos e garantias fundamentais do acusado. Insta esclarecer, contudo, que, ao longo dos anos, a doutrina e a jurisprudência passaram a mitigar a proibição das provas ilícitas, na tentativa de afastar eventuais distorções que a rigidez da exclusão poderia gerar, em hipóteses de excepcional gravidade. Tal posicionamento encontra embasamento no princípio da proporcionalidade, que autoriza a avaliação das provas ilícitas em casos de extrema gravidade, tendo em vista que nenhuma liberdade pública pode ser considerada de natureza absoluta. No que tange à incidência do princípio da proporcionalidade em favor do réu, por exemplo, não há dúvidas de sua aplicação, sendo pacífico, na jurisprudência, o entendimento de que, em tais hipóteses, a ilicitude é eliminada por causas excludentes, diante da prevalência do princípio da inocência. Já as provas ilícitas por derivação são aquelas lícitas em si mesmas, mas produzidas a partir de um fato ilícito. Em que pese o atual entendimento majoritário do Supremo Tribunal Federal, que, na esteira do raciocínio desenvolvido pela teoria dos frutos da árvore envenenada, considera que a prova ilícita originária é capaz de contaminar as demais provas dela decorrentes, posiciono-me na trincheira daqueles que defendem que o mero fato de não se admitir as provas ilícitas em juízo não possui o efeito de gerar a nulidade de todo o processo, eis que a Lei Maior não afirma serem nulos os processos, em que exista alguma prova obtida por meios ilícitos. Logo, se uma prova ilícita ou ilegítima revela-se necessária para evitar uma condenação injusta, como visto anteriormente, deverá ser agasalhada. Nesses casos, se a prova se retrata imprescindível deve ser admitida, por adoção do princípio da proporcionalidade” (http://www.amb.com.br/portal/index.asp?secao=artigo_detalhe&art_id=318).

endereços eletrônicos. É de suma importância observar também os horários GMT (*Greenwich Mean Time*), de acordo com o horário oficial de Brasília ou onde a pessoa estiver geograficamente localizada.

A natureza jurídica da prova é a forma pela qual se apura a verdade em juízo (instituto do direito processual). Trata-se de um meio usado pelas partes para atingir um resultado.

Segundo Pedro Batista Martins, prova é “o conjunto de elementos de que se serve o juiz para formar a convicção sobre os fatos em que se funda a demanda”¹³⁷.

Um dos princípios do contrato eletrônico é o do não repúdio, ou seja, é inválida qualquer alegação no que cinge ao suporte do contrato. Como contrato eletrônico “é um documento eletrônico”, seria ilógico não aplicarmos o mesmo princípio ao documento eletrônico e conseqüentemente ao seu valor probatório.

O Código Civil, em seu art. 225, *in verbis*, afirma que “as reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, lhes impugnar a exatidão”.

E o art. 332 do Código de Processo Civil assegura que “todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa”.

Logo a seguir o art. 334, do mesmo diploma legal, é bastante claro ao determinar que: “Não dependem de prova os fatos: (...) IV — em cujo favor milita presunção legal de existência ou de veracidade”¹³⁸.

Ambos os diplomas legais aceitam, portanto, o documento eletrônico como prova. O Código de Processo Penal também segue no mesmo sentido: “Salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo” (art. 231). E continua no art. 232: “Consideram-se documentos quaisquer escritos, instrumentos ou papéis, públicos ou particulares”.

Além de não existir nenhum óbice jurídico, o documento eletrônico assinado digitalmente torna factível a visualização de qualquer tentativa de modificação do documento por meio da alteração da sequência binária.

Cumprе destacar também a Medida Provisória n. 2.200/2001 que institui

137. MARTINS, Pedro Batista. *Comentários ao Código de Processo Civil*. v. 2, p. 383.

138. Ressalte-se que este artigo é o utilizado quando se faz uso de uma assinatura digital dentro do padrão da ICP-Brasil (MP 2.200/01) — ver mais detalhes no item 8.15 sobre Assinatura Digital e Certificação Digital.

a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), cuja finalidade é descrita em seu art. 1º “para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras”.

Na referida Medida Provisória, mais especificamente no art. 10, § 1º, consta a presunção de veracidade dos documentos eletrônicos com o uso de processo de certificação disponibilizados pelo ICP-Brasil. Os documentos assinados dessa forma têm valor probante *erga omnes*¹³⁹.

A fotografia digital (documento eletrônico) não foi tratada pelo Código de Processo Civil, que, em seu art. 385, afirma: “A cópia de documento particular tem o mesmo valor probante que o original, cabendo ao escrivão, intimadas as partes, proceder à conferência e certificar a conformidade entre a cópia e o original. § 1º Quando tratar de fotografia, esta terá de ser acompanhada do respectivo negativo”.

Não obstante o fato de a fotografia digital não possuir negativo, há um arquivo eletrônico que representa o original; este também passível, assim como o negativo, de se submeter a um exame pericial que comprove a sua autenticidade.

Segundo Miguel Pupo Correia¹⁴⁰, “a eficácia jurídica dos documentos em geral e dos documentos eletrônicos em especial está, como já dissemos, fortemente dependente da confiança, credibilidade ou fiabilidade que possam merecer como reproduções — melhor se diria revelações — factos ou objectos, o que depende essencialmente de dois fatores: genuinidade e segurança. É genuíno o documento quando não sofreu alterações. É seguro tanto mais quanto mais difícil for alterá-lo e mais fácil de descobrir as alterações que tenha sofrido e reconstituir o texto original”.

Colaborando, ainda, cabe ressaltar a declaração categórica do art. 365 do Código de Processo Civil, ao dispor que: “Fazem a mesma prova que os originais: (...) II — os traslados e as certidões extraídas por oficial público, de instrumentos ou documentos lançados em suas notas”.

É bastante oportuno destacar que a nossa Constituição Federal adotou o Princípio do Livre Convencimento Motivado, e, por consequência, o mesmo ocorre com a legislação processual. O art. 131 do Código de Processo Civil¹⁴¹

139. No mesmo sentido o Código de Processo Civil: “Art. 334. Não dependem de prova os fatos: I — notórios; II — afirmados por uma parte e confessados pela parte contrária; III — admitidos, no processo, como incontroversos; IV — em cujo favor milita presunção legal de existência ou de veracidade”.

140. www.di.fc.ul.pt/~mpc/ — Acesso em 21-7-2008.

141. Em sentido contrário segue o sistema jurídico norte-americano, em que há uma

reza: “O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convencimento”.

Em seguida no art. 154 do mesmo codice pode-se ler que: “Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exigir, reputando-se válidos os que, realizados de outro modo, lhe preenchem a finalidade essencial.

Parágrafo único. Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil¹⁴².

Determina o inciso I do art. 389 do Código de Processo Civil que incumbe o ônus da prova, quando se tratar de falsidade de documento, à parte que a arguir.

Já no âmbito do Direito Processual Penal, “a letra e firma dos documentos particulares serão submetidas a exame pericial, quando contestada a sua autenticidade” (CPP, art. 235)¹⁴³.

estrutura hierárquica entre as provas. São elas:

Real evidence — consiste em evidências materiais, que podem literalmente ser trazidas à corte, como, por exemplo, arma de um crime, objetos físicos em geral.

Documentary evidence — evidência documental. Divide-se em:

a) *best evidence rule* — quando um documento é levado a juízo, o original deve ser apresentado.

b) *parol rule* — quando um documento é assinado por duas partes, apenas o que está escrito é válido, ou seja, nenhum acordo verbal pode modificá-lo.

Testimonial evidence — testemunhas de fatos.

Caso — *Breaking the neck*

<http://www.crn.com/components/weblogs/article.jhtml?articleId=173602157>.

142. A Lei n. 11.280/2006 inclui parágrafo único ao art. 154 do CPC, ficando, então, os Tribunais autorizados a regulamentar a comunicação eletrônica nos atos processuais, desde que utilizando os requisitos de segurança jurídica do ICP-Brasil. A norma é importantíssima, o que faltava para viabilizar o peticionamento eletrônico.

Entre as “*Best Practices*” podemos destacar: Serviço secreto americano — http://www.secretservice.gov/electronic_evidence.shtml

NHTCU — <http://www.nhtcu.org/>

NIST — <http://www.it.nist.gov/lab/bulletins/bltnnov01.htm>

USA Department of Justice — <http://www.cybercrime.gov/s&smanual2002.htm>

143. Resumo dos artigos relacionados:

Código de Processo Civil

Art. 131. O juiz apreciará livremente a prova, atendendo aos fatos e circunstâncias constantes dos autos, ainda que não alegados pelas partes; mas deverá indicar, na sentença, os motivos que lhe formaram o convencimento (Princípio do Livre convencimento Motivado).

Art. 154. Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exigir, reputando-se válidos os que, realizados de outro modo, lhe preenchem a finalidade essencial.

Parágrafo único. Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil.

Art. 332. Todos os meios legais, bem como moralmente admitidos legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa.

Art. 334. Não dependem de prova os fatos:

IV — em cujo favor milita presunção legal de existência ou de veracidade.

Art. 365. Fazem a mesma prova que os originais:

(...)

II — os traslados e as certidões extraídas por oficial público, de instrumentos ou documentos lançados em suas notas.

Medida Provisória n. 2.200

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiras em relação aos signatários, na forma do art. 131 da Lei n. 3.071, de 1º de janeiro de 1916 — Código Civil.

Código Civil

Art. 104. A validade do negócio jurídico requer: I — agente capaz; II — objeto lícito, possível, determinado ou determinável; III — forma prescrita ou não defesa em lei.

Comentários: O contrato eletrônico como negócio jurídico bilateral é plenamente válido segundo o ordenamento vigente.

Art. 107. A validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir.

Art. 141. A transmissão errônea da vontade por meios interpostos é anulável nos mesmos casos em que o é a declaração direta.

Art. 212. Salvo o negócio a que se impõe forma especial, o fato jurídico pode ser provado mediante: (...) II — documento;

Art. 215. A escritura pública, lavrada em notas de tabelião, é documento dotado de fé pública, fazendo prova plena.

Art. 216. Farão a mesma prova que os originais as certidões textuais de qualquer peça judicial, do protocolo das audiências, ou de outro qualquer livro a cargo do escrivão, sendo extraídas por ele, ou sob a sua vigilância, e por ele subscritas, assim como os traslados de autos, quando por outro escrivão consertados.

Art. 217. Terão a mesma força probante os traslados e as certidões, extraídos por tabelião ou oficial de registro, de instrumentos ou documentos lançados em suas notas.

Art. 219. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários.

Como foi descrito anteriormente, existe ainda a possibilidade, caso o documento eletrônico não tenha sido assinado, ou o certificado não esteja vinculado ao ICP-Brasil, de se verificar a autenticidade e integridade do documento eletrônico por meio da devida perícia nos computadores. Foram criadas normas de boas práticas para coleta dessas evidências.

Em virtude do uso massivo de computadores, a evidência eletrônica pode e deve ser utilizada, como mencionamos anteriormente, mesmo que ela não esteja assinada digitalmente, pois, na verdade, há níveis de evidência, das mais fortes e não repudiáveis às mais frágeis e questionáveis (v. os casos de apreensão de computadores, seja para qual fim for — penal, civil, tributário... —, em que as informações constantes no disco rígido, caso não sejam provas em si, são ao menos um norte).

Todavia, nunca alcançaremos a certeza inequívoca de confiabilidade, tanto no sistema eletrônico quanto no tradicional, ou em outro qualquer, mas, ainda assim, é possível imprimir uma confiabilidade necessária para a concretização de negócios jurídicos nesses meios.

Podemos afirmar que a tecnologia trouxe mais ferramentas para validação jurídica das provas, algo que se busca há muito, e hoje, por certo, já há força legal muito maior numa prova composta por um *e-mail* do que apenas um testemunho oral ou um mero fax; o mesmo para uma assinatura digital ou biométrica do que apenas o número de um RG ou CPF anotados a mão sem conferência do documento, ou cuja foto, normalmente, está desatualizada. Afinal, para todos nós, o teste de DNA continua sendo considerado prova inequívoca de autoria, apesar de não ter lei e não ser 100% de certeza.

Neste sentido, é recomendável, de forma complementar, a leitura do item 8.17, sobre Computação Forense, que é a ciência responsável pelo manuseio, coleta e análise das evidências eletrônicas.

Parágrafo único. Não tendo relação direta, porém, com as disposições principais ou com a legitimidade das partes, as declarações enunciativas não eximem os interessados em sua veracidade do ônus de prová-las.

Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

Art. 889. (...)

§ 3º O título poderá ser emitido a partir dos caracteres criados em computador ou meio técnico equivalente e que constem da escrituração do emitente, observados os requisitos mínimos previstos neste artigo.

Código de Processo Penal

Art. 157. O juiz formará sua convicção pela livre apreciação da prova.

8.17. Assinatura digital e certificação digital

Para que seja possível avançar na questão de Assinatura Digital e Certificação Digital, primeiramente se deve entender conceitualmente o que é criptografia. A origem da certificação digital está na criação de uma tecnologia de criptografia patenteada em 1983 por professores do Instituto de Tecnologia de Massachusetts (MIT), nos Estados Unidos.

A criptografia¹⁴⁴ não é algo novo para o nosso ordenamento jurídico, nem no dia a dia das pessoas, já que toda vez que é utilizado algum tipo de código ou cifragem de comunicação (inclusive as anotações de uma adolescente que faz uso de troca de letras para não permitir a leitura por terceiros de suas anotações).

144. Para entender melhor o conceito, aqui estão algumas definições da Doutrina e da Jurisprudência:

“O consumidor deve ter conhecimento que existe um sistema moderno, já adotado em outros países, denominado criptografia, e só com ele é possível controlar a autenticidade e a veracidade de informações contidas nas cláusulas do documento eletrônico... Sem o uso da assinatura criptográfica, não se obtém documento eletrônico com força de prova em juízo” (Ruy Rosado de Aguiar, Ministro do Supremo Tribunal de Justiça — citado pela Ag. Estado).

“Criptografia é a técnica utilizada para garantir o sigilo das comunicações em ambientes inseguros ou em situações conflituosas. Atualmente, sua aplicação se expandiu para além do mero sigilo, tornando-se um elemento essencial na formação de uma infraestrutura — PKI — para o comércio eletrônico e a troca de informações” (Regis Magalhães Soares de Queiroz).

“(…) Código Brasileiro de Trânsito. Imposição de multa. Discussão sobre existência e/ou validade da notificação de que trata o artigo 281, parágrafo único, inciso II, da Lei 9.503/97. Suficiência da prova eletrônica da remessa da correspondência em nome do proprietário e ao endereço declarados no registro do veículo. Exegese das Súmulas 127 e 312, do Eg. STJ. Ato administrativo com presunção de legitimidade e veracidade. Suporte doutrinário. Apelação não provida neste tema específico. (...)” (TJSP, Apelação 9203383-44.2003.8.26.0000, rel. Fermino Magnani Filho, j. 14-3-2011).

“Inépcia da inicial. Preliminar rejeitada por decisão de saneamento do feito da qual não se insurgiu o autor. Preclusão consumada. Preliminar afastada. Incompetência em razão da matéria. Preliminar afastada em primeiro grau através de despacho saneador. Matéria de ordem pública. Conhecimento. Alegação de competência da Vara de Família para julgamento do feito em razão da existência de união estável entre autora e réu. Pretensão inicial que não diz respeito a reconhecimento ou dissolução da sociedade conjugal. Preliminar rejeitada. Cerceamento de defesa. Preliminar apreciada através de decisão interlocutória. Oferecimento de agravo de instrumento pelo réu. Decisão que negou seguimento ao recurso interposto. Preclusão consumada. Preliminar afastada. Ação de cobrança. Empréstimo feito ao réu através de depósitos bancários. Réu revel. Alegação de tratar-se de doação que não restou comprovada. Mensagem via documento eletrônico (*e-mail*) confessando a existência da dívida enviado à autora não impugnado em contestação. Presunção de veracidade dos fatos narrados na inicial que não foi elidida por prova em contrário. Sentença mantida. Art. 252, do RITJESP. Recurso improvido” (TJSP, Apelação 0125971-11.2008.8.26.0100, rel. Des. Ligia Araújo Bisogni, j. 14-9-2011).

Em termos técnicos, a criptografia é uma ferramenta de codificação usada para envio de mensagens seguras em redes eletrônicas. É muito utilizada no sistema bancário e financeiro. Na Internet, a tecnologia de criptografia utiliza o formato assimétrico, ou seja, codifica as informações utilizando dois códigos, chamados de chaves, sendo uma pública e outra privada para decodificação, que representam a assinatura eletrônica do documento. No Brasil, o sistema já utiliza duas chaves, pública e privada, de 128 *bits*¹⁴⁵.

A assinatura eletrônica é, portanto, uma chave privada, ou seja, um código pessoal e irreproduzível que evita os riscos de fraude e falsificação. Para o Direito Digital, uma chave criptográfica significa que o conteúdo transmitido só pode ser lido pelo receptor que possua a mesma chave e é reconhecida com a mesma validade da assinatura tradicional.

A tendência é a tecnologia ser aprimorada para aumentar o nível de segurança na rede (que, em tese, já é maior do que o que se tem no mundo real, em que a possibilidade de ter uma assinatura falsificada graficamente é maior). É importante ressaltar que a assinatura eletrônica é mais segura que a real, pois é certificada, “autenticada”, ou seja, verificada em tempo real no sistema de duas chaves, enquanto as assinaturas tradicionais não são verificadas imediatamente e muitas nem sequer são verificadas, como acontece muito com cheques e cartões de crédito.

A assinatura digital possibilita o reconhecimento da origem de um ato e também identifica um usuário aceito e permitido em determinada transação. Um exemplo cotidiano é seu uso em empresas com redes de computadores interligados: as senhas de segurança limitam ou abrem o acesso de certos funcionários a determinadas áreas da empresa; analogicamente, é como se só alguns funcionários tivessem as chaves de determinadas salas da sede física da empresa, só que aqui estamos falando de dados virtuais.

Apesar de o Brasil ser bastante avançado na área tecnológica de criptografia, nossa legislação está em uma fase de adaptação constante da regulamen-

145. Legislação Brasileira sobre Autoridades Certificadoras e Criptografia: Instrução Normativa SRF n. 462, de 19 de outubro de 2004; Instrução Normativa SRF n. 580, de 12 de dezembro de 2005; Decreto n. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal; Decreto n. 4.176, de 28 de março de 2002, o qual informa que as propostas de projetos de ato normativo serão encaminhadas à Casa Civil por meio eletrônico. Decreto n. 3.587, de 5 de setembro de 2000, revogado pelo Decreto n. 3.996, de 31 de outubro de 2001, que dispõe sobre a utilização de Assinaturas Digitais e o Desenvolvimento da Infraestrutura de Chave Pública para as entidades da Administração Pública Federal.

tação da assinatura e da certificação virtuais¹⁴⁶. Tentar definir a quem serão dadas essas atribuições — ou seja, quem serão e como funcionarão os cartórios virtuais — é o mesmo que burocratizar um meio de comunicação cujo principal propósito é a agilidade¹⁴⁷, por isso não é questão de definir o “local” em que será feito o reconhecimento das “firmas”, as senhas ou assinaturas virtuais, uma vez que em ambiente virtual e com o *software* adequado isto pode ser feito automaticamente na rede verificando em uma conexão sua origem e seu receptor, reconhecendo ambos e gravando a operação para fins de necessidade de investigação se houver qualquer problema.

Na parte pública, o Governo já tem a solução para fazer licitações virtuais¹⁴⁸, compondo uma base de dados de empresas que têm suas “firmas” reconhecidas para esse tipo de operação, assim como funciona um banco de dados de registro prévio de qualquer empresa que queira prestar serviços ou vender produtos ao governo.

Hoje, os brasileiros possuem a opção de utilizar para diversas finalidades a certificação digital, uma tecnologia já disseminada em países da Europa e nos Estados Unidos, que confere segurança às informações que trafegam na rede, mitigando o risco de serem interceptadas e garantindo a autenticidade dos documentos virtuais, uma vez que já não existe a dúvida sobre quem os enviou.

Outros exemplos que demonstram a praticidade e vantagens do uso do certificado digital estão na sua aplicabilidade junto aos órgãos do governo como

146. Medida Provisória n. 2.200, de 28 de junho de 2001 — Institui a Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil, e dá outras providências; Decreto n. 3.872, de 18 de julho de 2001 — Dispõe sobre o Comitê Gestor de Infraestrutura de Chaves Públicas Brasileira (CG ICP-Brasil) e dá outras providências; Decreto n. 3.996, de 31 de outubro de 2001 — Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

147. A Ordem dos Advogados do Brasil (OAB) lançou o seu Certificado Digital no dia 14 de outubro de 2002, quando foi gerada a chave-raiz da Infraestrutura de Chaves Públicas da OAB (ICP-OAB). Desde então, vem sendo feita a emissão de certificados eletrônicos para advogados de todo o País. Outros passos importantes também foram dados, como a oferta gratuita do sistema de certificação gerado pela ICP-OAB ao Superior Tribunal de Justiça e a realização de convênios de cooperação para desenvolvimento tecnológico com Tribunais de Justiça estaduais. Esses convênios têm como objetivo agilizar as atividades relacionadas às rotinas processuais e criar condições para que o Judiciário avance rumo à criação do processo eletrônico. Site: <<http://cert.oab.org.br>>.

148. Essas licitações são reguladas pela Lei n. 10.520, de 17 de julho de 2002, que institui, no âmbito da União, nos termos do art. 37, XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e pelo Decreto n. 3.555, de 8 de agosto de 2000, que aprova o regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

a Receita Federal, em que o contribuinte, por meio do e-CPF, pode receber mensagens da Receita sobre os trâmites de sua declaração do imposto de renda, bem como corrigir erros *online*. No meio burocrático, fica dispensada a visita ao cartório em diversas situações, como, por exemplo, para autenticar contratos de compra e venda de imóveis, validar documentos de concorrência pública, entre outros. Para o comércio eletrônico, do ponto de vista do comprador, uma empresa que possui uma assinatura digital confere credibilidade ao negócio efetuado na Internet. Destacamos ainda seu papel no uso de *e-mail*, junto ao Poder Judiciário e nas instituições financeiras.

Vale notar que o Brasil é um dos únicos países do mundo a exigir o reconhecimento de firmas para documentos oficiais. Nos Estados Unidos, a assinatura eletrônica foi regulamentada¹⁴⁹, oferecendo garantias ao consumidor. Assim, o consumidor é protegido, por exemplo, da ação de alguém que pode insinuar que o avisou do vencimento de um título, sem que isso tenha sido registrado eletronicamente.

Mais uma vez, deve-se ter em mente que não há como ter 100% de garantia de segurança, nem no mundo real nem no mundo virtual. Vejamos o que ocorre com os golpes em caixas eletrônicos de Bancos. Mas sabemos que a tecnologia permite ampliar essa segurança para limites adequados à manutenção da paz social, devendo cada um, individualmente, zelar e ser responsável pela segurança de suas senhas de modo a ajudar a coibir tais práticas, cada vez mais comuns.

8.18. Aspectos legais da biometria

A Constituição Federal de 1988 (CF), no capítulo que trata *dos Direitos e Deveres Individuais e Coletivos* (Cap. I do Título II), art. 5º, X, descreve: “*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas*”.

Dessa forma, temos três conceitos principais a serem tratados no presente caso: a intimidade, a privacidade e a imagem.

149. A primeira lei a regulamentar a assinatura digital nos Estados Unidos foi a *Utah Digital Signature Act*, promulgada em 1995 pelo Estado de Utah, e se limitava a dispor sobre assuntos relacionados a assinaturas digitais baseadas na criptografia. Como, atualmente, a maioria dos Estados americanos já possui normas para assinaturas digitais, fez-se necessária, então, a criação de uma lei federal para promover a harmonia delas e, em 19 de novembro de 1999, o *Millennium Digital Commerce Act* foi promulgado pelo Congresso. Hoje, já está em vigor o *Electronic Signatures in Global and National Commerce Act*, que aborda, além do tema das assinaturas eletrônicas no comércio entre estados e países, pontos importantes como direitos do consumidor, contratos e arquivos eletrônicos e regras para notarizar e autenticar os documentos.

A intimidade, segundo Félix Ruiz Alonso “é o âmbito interior da pessoa mais profundo, mais recôndito, secreto ou escondido dentro dela. É, assim, algo inacessível, invisível, que só ela conhece, onde ela só elabora ou constrói livremente seu próprio agir e onde se processa sua vida interior”¹⁵⁰.

A intimidade é um “estágio” pré-jurídico, pois esta, em razão de seu caráter originário, antecede o Direito, e o fundamento da pessoa está calcado na intimidade, ou seja, sem a intimidade não haveria de se falar em sujeito de direito. A pessoa, portanto, tem seu mundo íntimo protegido pelo Direito, da mesma forma que resguarda o nascituro antes de nascer.

Já a privacidade se encontra dentro da seara jurídica. Ato posterior à intimidade, tem relevância e estreita relação com o Direito.

A vida privada, como descrito na Constituição Federal, ou a privacidade, segundo José Afonso da Silva, é “o conjunto de modo de ser e viver, como direito de indivíduo viver sua própria vida”¹⁵¹.

Segundo José Afonso da Silva, “a privacidade também pode ser entendida como o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso ser legalmente sujeito”.

Outro termo trazido pelo art. 5º, X, é “a imagem das pessoas”, sendo que conforme também leciona José Afonso da Silva, “a inviolabilidade da pessoa consiste na tutela do aspecto físico, como é *perceptível visivelmente*”¹⁵².

Em sentido contrário, temos a definição de Hermano Duval: “Direito à imagem é a projeção da personalidade física (traços fisionômicos, corpo, atitudes, gestos, sorrisos, indumentárias, etc.) ou moral (aura, fama, reputação, etc.) do indivíduo (homens, mulheres, crianças ou bebês) no mundo exterior”¹⁵³. De maneira bastante similar também é o entendimento de Walter Moraes, que definiu imagem como “toda sorte de representação de uma pessoa”¹⁵⁴.

Segundo Aurélio Buarque de Holanda, imagem é “aquilo que evoca uma determinada coisa, por ter com ela relação simbólica; símbolo”¹⁵⁵. Dessa forma,

150. ALONSO, Félix Ruiz. *Direito à privacidade*. São Paulo: Ideias e Letras, 2005.

151. SILVA, José Afonso da. *Direito constitucional positivo*. 10. ed. São Paulo: Malheiros, 1994. p. 204.

152. SILVA, José Afonso da. Op. cit.

153. DUVAL, Hermano. *Direito à imagem*. São Paulo: Saraiva, 1988. p. 105.

154. MORAES, Walter. *Direito à própria imagem*. São Paulo: Saraiva, 1977. p. 742.

155. FERREIRA, Aurélio Buarque de Holanda. *Imagem*. In: *Pequeno dicionário da língua portuguesa*, p. 742.

compreende-se imagem não apenas como o semblante da pessoa, mas também partes distintas de seu corpo.

Biometria, portanto, pode ser definida como “*use of measurable physiological characteristics to authenticate a user such as fingerprints or facial characteristics*”, isto é, o uso de característica fisiológica mensurável para autenticar um usuário, como impressão digital ou reconhecimento facial¹⁵⁶.

Expostos os conceitos, surgem as seguintes questões: o dado biométrico goza de alguma privacidade? Ou ainda há a incidência de direito de imagem?

Dirimindo a hipótese de entendimento conflituoso entre os termos, sobre a privacidade como estágio posterior à intimidade, há a escolha do sujeito na renúncia parcial do sigilo de aspectos de sua vida cotidiana, ainda que haja o desejo de resguardo a determinado círculo, ou seja, de sua não publicidade. Nesse sentido aproveitamos a lição de Tércio Sampaio Ferraz:

“A vida privada pode envolver, pois, situações de opção pessoal (como a escolha do regime de bens no casamento), mas que, em certos momentos, podem requerer a comunicação a terceiros (na aquisição, por exemplo, de um imóvel). Por aí ela difere da intimidade, que não experimenta esta forma de repercussão”¹⁵⁷.

Tomando como certo, o fato de que a coleta de dados biométricos recai sobre o direito à privacidade, não há que discutir sobre a possibilidade de invasão, haja vista que tal processo somente será realizado mediante a autorização do indivíduo proprietário da característica captada, seja ela o dedo polegar ou olho, por exemplo, os quais por motivos óbvios são intransferíveis a terceiros.

Analogicamente qualquer problemática intrínseca ao direito de imagem, previsto no mesmo excerto da Carta Magna, dada a captura do espectro visível a olho nu do corpo humano, como no reconhecimento de face, deverá ser compreendida da mesma forma, pois uma vez que há a autorização expressa do usuário, inclusive declarada e assinada em Termo, será afastada qualquer discussão sobre uma possível não conformidade legal.

Ainda, quanto ao direito de imagem, pode-se arguir que a questão não é pacífica, pois segundo conceitua José Afonso da Silva, o referido direito está atrelado ao aspecto físico, como destacamos: “*perceptível visivelmente*”, o que não é factível de ocorrer por meio da estrutura de veias¹⁵⁸ da mão de um indi-

156. Tradução nossa.

157. FERRAZ, Tércio Sampaio. Sigilo de dados: direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito de São Paulo*, 1993.

158. Utilizamos este exemplo porque esta será a tecnologia implementada pelo Banco Bradesco.

víduo. Ou seja, não há possibilidade nenhuma de uma pessoa, apenas mediante o dado biométrico, identificar outra pessoa.

Mas, se analisarmos por meio dos conceitos de Hermano Duval e de Walter Moraes, há incidência do direito de imagem, pois o primeiro atesta que “Direito à imagem é a projeção da personalidade física”, enquanto o segundo conceitua-o como “toda sorte de representação de uma pessoa”.

Alusivo à concessão de direitos, é importante fazer a analogia com o genoma de um indivíduo, que também é suscetível à concessão. Nesse diapasão, destaca Maria Helena Diniz: “Para salvaguardar a intimidade da pessoa, a análise completa do genoma somente poderá dar-se com o expresse e prévio consentimento informado de pessoa maior e capaz”¹⁵⁹.

Então, se o indivíduo capaz pode conceder o uso de seu genoma, que é a imagem científica de sua pessoa, não faz sentido restringir a concessão de um simples dado biométrico.

Portanto, é recomendável que as empresas que queiram fazer uso de processos de biometria implementem e colham assinatura de seus funcionários e/ou usuários em um documento específico de “Termo de Concessão” referente aos dados biométricos que serão coletados e armazenados, ressaltando o fato de que as informações de menores somente poderão ser colhidas mediante a autorização dos pais ou representantes legais, mediante a assinatura do termo de concessão.

Devemos destacar, por oportuno, que o tempo de guarda deve ser sempre determinado, ou seja, após o encerramento da relação entre as partes, a empresa deve eliminar os dados biométricos coletados, por se tratar de direito relacionado à personalidade (direito de imagem, privacidade), a não ser que alguma situação justifique a guarda deles.

Logo, como medida de cautela, pode ser estabelecido um prazo para guarda dos dados que considere um tempo mínimo necessário caso haja eventual discussão judicial ou extrajudicial em que estes sirvam como prova ou sejam objeto de repúdio. Atendendo ao Código Civil, tal prazo pode variar entre três a cinco anos.

Outro ponto polêmico estaria no próprio arquivamento dos “templates” biométricos, uma vez que a Lei n. 8.078, de 11 de setembro de 1990, o Código de Defesa do Consumidor (CDC), não impede a elaboração e/ou manutenção de banco de dados e do cadastro de clientes; entretanto este deverá:

- Ser comunicado em sua abertura por escrito ao consumidor, quando não solicitada por ele;
- Ser acessível ao consumidor;
- Ser objetivo, claro, verdadeiro e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos; e
- Ser imediatamente corrigido, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas, sempre que o consumidor encontrar qualquer inexactidão nos seus dados e cadastros.

Desde que não haja abuso ou desrespeito a tais quesitos previstos no art. 43 do CDC, estará a empresa receptora dos dados plenamente autorizada a manter sob sua guarda tal base cadastral.

O Código de Defesa do Consumidor, em seu art. 6º, III, estabelece o seguinte:

“Art. 6º São direitos básicos do consumidor:

(...)

III — a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade e preço, bem como sobre os riscos que apresentem”.

Os dados biométricos, assim como os demais, gozam da mesma proteção, como já destacamos acima. Portanto, recomendamos que as empresas, especialmente as instituições financeiras, apliquem o disposto na norma ISO/IEC 27002 (antiga 17799-2005), item 15.1.4, que trata da proteção de dados e privacidade de informações pessoais.

Do ponto de vista da regulamentação sobre biometria, há diversas normas internacionais que tratam da matéria, especialmente no tocante ao seu uso no mercado financeiro¹⁶⁰.

160. Algumas normas internacionais sobre biometria:

— ANSI X9.84-2003 — Biometric — Information Management and Security for the Financial Services Industry;

— ISO/IEC 19795-1:2006 — Information technology — Biometric performance testing and reporting — Part 1: Principles and framework;

— BIP 0012 — Data Protection Guide;

— ISO/IEC 15408 — 1 Evaluation Criteria for IT security (Introduction and General

159. DINIZ, Maria Helena. *Direito à privacidade*. São Paulo: Ideias e Letras, 2005. p. 73.

Como com qualquer tecnologia, há benefícios, mas, por sua vez, também há, logicamente, inúmeros riscos que envolvem a execução, ou melhor, a implementação deste tipo de autenticação, dentre os quais podemos destacar alguns: por exemplo, caso um usuário sofra um acidente justamente na mão que está cadastrada, como ele deverá proceder? O ideal é que o indivíduo seja orientado, previamente, pela empresa por um meio de comunicação adequado, devendo ser previstas hipóteses de contingência e continuidade no tocante à disponibilidade do acesso. Finalmente, é imprescindível destacar que, em qualquer uma das hipóteses acima mencionadas, a impossibilidade de realização de uma transação, de qualquer espécie, ocasionada em virtude de falhas em qualquer fase do sistema de biometria responsabilizará a empresa por qualquer dano causado ao cliente, tendo em vista a notoriedade de que o processo de análise de dados biométricos baseia-se em proximidade, não em exatidão, e de que o risco de falha é inerente à sua natureza, condicionada a padrões fisiológicos humanos razoavelmente voláteis.

8.19. Computação forense e a perícia digital

Segundo pesquisas atuais, crescem os crimes virtuais¹⁶¹, e estes, em breve, irão ultrapassar os crimes físicos¹⁶². Sendo assim, podemos vislumbrar a impor-

Model), ISO/IEC 15408 — 2 Evaluation Criteria for IT security (Security Functional Requirements), ISO/IEC 15408 — 3 Evaluation Criteria for IT security (Security Assurance Requirements).

— ISO/TR 17944 Banking — Security and other Financial Service — Framework for Security in Financial Systems, que já foi aprovada (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=33285).

161. O Orkut concentra 90% das 56 mil denúncias recebidas nos últimos dois anos pela Central Nacional de Crimes Cibernéticos, referentes à divulgação de material pornográfico infantil no Brasil por meio da internet. (fonte <http://www.aasp.org.br/aasp/imprensa/clipping/cli_noticia.asp?idnot=3412> e <<http://portal.rpc.com.br/gazetadopovo/vidaecidadania/conteudo.phtml?tl=1&id=786313&ct=Cibercriminosos-agem-sem-medo>>).

Em 10 anos, 90% dos crimes serão pela internet. Fonte: <<http://www.tvcanal13.com.br/noticias/em-10-anos90dos-crimes-serao-pela-internet-25720.asp>>.

O Brasil é o país com maior incidência de crimes eletrônicos. O Brasil foi o principal país em atividade nociva na América Latina durante o segundo semestre de 2007, respondendo por 37% do total. O Brasil foi o país com a maior percentagem de computadores infectados por *bot* na região no segundo semestre de 2007, com 40% do total. Durante o segundo semestre de 2007, 36% de todos os *spams* detectados na América Latina foram originados no Brasil. São Paulo é a 5ª cidade da América Latina com maior número de computadores infectados por *bot* no 2º semestre de 2007 (Fonte: Relatório de Ameaça à Segurança na Internet — abril/2008 — Symantec).

162. Mais detalhes sobre a pesquisa podem ser obtidos no link: <http://www.crime-rese->

tância que a computação forense terá para a sociedade, pois é por meio dessa ciência que será possível descortinar os fatos e punir os infratores.

Da mesma forma que as demais ciências que estudam o crime, a computação forense está inserida na ciência criminalística, que pode ser definida como uma “*disciplina autônoma, integrada pelos diferentes ramos do conhecimento técnico-científico, auxiliar e informativa das atividades policiais e judiciais de investigação criminal, tendo por objeto o estudo dos vestígios materiais extrínsecos à pessoa física, no que tiver de útil à elucidação e à prova das infrações penais e, ainda, à identificação dos autores respectivos*”¹⁶³.

Já a ciência forense pode ser definida como: “*A aplicação de princípios das ciências físicas ao Direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade*”¹⁶⁴.

A computação forense, então, consiste no uso de métodos científicos na preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais.

A ciência forense busca desvendar seis elementos: *Quem?*, *O quê?*, *Quando?*, *Como?*, *Onde?* e *Por quê?*.

Em outras palavras, o escopo do exame forense é a extração de informações de qualquer vestígio relacionado com o caso investigado que permitam a formulação de conclusões acerca da infração. No universo da criminalística, vestígio é qualquer marca, fato, sinal ou material, que seja detectado em local onde haja sido praticado um fato delituoso. Indício, segundo o art. 239 do Código de Processo Penal, é “*a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outra ou outras circunstâncias*”¹⁶⁵.

Logo, a evidência digital é toda a informação ou assunto criada e sujeita, ou não, a intervenção humana, que possa ser extraída de um computador ou de qualquer outro dispositivo eletrônico. Além disso, a evidência digital sempre deverá estar em formato de entendimento humano.

arch.org/news/02.06.2006/1804/ (acesso em 21-7-2008).

163. TOCHETTO, D.; GALANTE, H.; ZARZUELA, J. *Tratado de perícia criminalística*.

164. *Manual de patologia forense* do Colégio de Patologistas Americanos, 1990.

165. NUCCI, Guilherme de Souza. *Código de Processo Penal comentado*, 4. ed., São Paulo, Revista dos Tribunais, 2005, p. 479.

Já o artefato representa os restos de uma atividade de ataque ou de um incidente que pode estar ou não ligado, por exemplo, a um invasor de sistemas, podendo ser desde o *software* usado por este indivíduo, até um código malicioso, os registros, os dispositivos de busca de vulnerabilidades e até mesmo uma coleção de ferramentas.

Toda investigação tem início com base nas evidências e informações coletadas. O meio virtual não diverge do físico, isto é, as evidências e informações existem desta vez em um disco rígido, celular, ou até mesmo no código-fonte de um arquivo malicioso.

Embora não esteja prevista na legislação processual brasileira uma hierarquia de provas¹⁶⁶, acaba existindo uma prevalência da prova pericial no conjunto probante. Tal preferência decorre do fato de a prova pericial ser produzida a partir de fundamentação científica, não dependendo de interpretações subjetivas. Nenhuma tecnologia, desde o advento do DNA, teve um efeito potencial tão grande em tipos específicos de investigações como a computação forense.

Os indícios que caracterizam a infração, ou relacionam o suspeito ao ato ilícito, são os arquivos de imagens de pornografia infantil, mensagens eletrônicas com ameaças ou chantagens, arquivos com informações incriminatórias ou dados roubados. Exemplos de locais em que podem ser encontrados tais indícios são: os sistema de arquivos, arquivos de *log*, espaços não utilizados no dispositivo de armazenagem, arquivos temporários, área de *swap*, setor de *boot*, memória, periféricos, comportamento de processos etc.

As cinco regras para a evidência eletrônica são: a **admissibilidade**, ou seja, ter condições de ser usada no processo; **autenticidade**, ser certa e de relevância para o caso; a **completude**, pois esta não poderá causar ou levar a suspeitas alternativas; a **confiabilidade**, não devem existir dúvidas sobre sua veracidade e autenticidade; e a **credibilidade**, que é a clareza, o fácil entendimento e interpretação.

Outra ciência que auxilia a computação forense é a *network forensic*, que se utiliza de arquivos de *log* para determinar fatos; início e término do acesso, quais *urls* foram acessadas, como foi o *log* na rede, de onde foi efetuado o acesso etc. A computação forense possui seus próprios termos, que devem ser estudados com o objetivo de se realizar perícias com elaboração de laudos que

166. Art. 157 do Código de Processo Penal: "O juiz formará sua convicção pela livre apreciação da prova".

tenham uma capacidade de compreensão única e uniforme. Por isso, deve-se usar o glossário padrão de nomenclaturas¹⁶⁷.

Apesar do alto nível de precisão da computação forense, há uma fragili-

167. Alguns termos do glossário padrão de nomenclaturas da Computação Forense:

— Arquivos de *log*: representam um papel importante na análise do sistema, pois permitem a reconstituição de fatos que ocorreram no sistema computacional. Variam de acordo com o sistema operacional, os aplicativos e serviços executados no sistema e as configurações determinadas pelo administrador. Registram, por exemplo: as atividades do usuário, dos processos e do sistema, as conexões de rede, as atividades da rede e informações específicas dos aplicativos e dos serviços.

— Espaços não utilizados no dispositivo de armazenagem: tais espaços podem conter indícios que o usuário tentou apagar. Entretanto, a "deleção" de arquivos e diretórios não apaga os dados do dispositivo de armazenagem, apenas disponibiliza o espaço ocupado para ser sobrescrito por novos arquivos. São caracterizados por espaços não alocados dentro do sistema de arquivos, espaços alocados a arquivos mas não totalmente utilizados e áreas do dispositivo de armazenagem que não constituem uma partição do disco ou que não contêm um sistema de arquivos.

— Arquivos temporários: alguns programas criam arquivos temporários durante sua execução, que são normalmente apagados automaticamente ao final da sessão de trabalho.

— Área de *SWAP*: é a área utilizada pelo gerenciador de memória do sistema operacional como uma grande área de armazenamento temporário, permitindo que processos sejam momentaneamente descarregados da memória principal, liberando espaço para execução de outros.

— Setor de *BOOT*: contém informações relativas aos programas que são carregados quando o computador é inicializado. Se tais informações forem modificadas, é possível carregar qualquer programa durante a inicialização do computador.

— Memória: armazena todo tipo de informação volátil, como, por exemplo, informações dos processos que estão em execução, dados que estão sendo manipulados e, muitas vezes, ainda não foram salvos no disco e informações do sistema operacional.

— Periféricos: dispositivos como *modems*, *paggers*, aparelhos de fax e impressoras. Contêm memórias que podem ser acessadas e salvas. Além disso, dispositivos não autorizados podem ser implantados no sistema operacional, possibilitando a execução da infração.

— Comportamento de processos: cada processo se executa em um ambiente com privilégios específicos que determinam quais recursos do sistema, programas e arquivos de dados podem ser acessados, e de que modo. Qualquer alteração nesse comportamento pode ser um indicador de interferência intencional. Um invasor pode desvirtuar a execução de um programa, causando sua falência, ou fazendo com que ele opere de maneira inesperada ao administrador ou usuário (acessando informações não autorizadas ou consumindo recursos excessivos, por exemplo).

— *Buffer overflow*: além de saber as fontes de busca o ideal é que o perito reconheça alguns elementos dos principais ataques realizados em ambientes computacionais, tais como o erro causado quando o programa tenta armazenar muitos dados na área de memória temporária e que pode ser explorado por *hackers* para executar códigos maliciosos.

— *Denial of Service*: método de ataque de negação de serviço a um computador ou rede que atenta contra o limite ou previne acesso para a Internet pela "inundação" de pedidos (para uma *webpage* ou recurso *online*) ou *e-mail* (causando sobrecarga no sistema). Uma variante desse ataque é conhecida como Negação de Serviço Distribuído, que se utiliza de múltiplos computadores, aumentando o tráfego e reduzindo as defesas da máquina vítima ou rede.

dade: a coleta das evidências. Coletar de forma errônea pode tornar ilícita ou inválida determinada prova. Também, ainda existe a possibilidade de alguma prova ilícita contaminar as demais, como ocorre na teoria dos frutos da árvore envenenada¹⁶⁸, eliminando todas as chances no litígio judicial.

Outro problema enfrentado pelas evidências digitais é a falta de confiança dos magistrados nesse tipo de prova. Logo, cabe ao perito retirar esse caráter dubio da evidência em um laudo pericial claro, e, como inexiste uma hierarquia de provas no Direito brasileiro, caberá ao juiz analisar e medir a importância das evidências.

Algumas recomendações para que o processo de computação forense seja realizado com perfeição são: não ligar o computador se a máquina já estiver desligada; tirar fotografias visíveis, de boa qualidade, dos elementos presentes no local, bem como do próprio local físico; remover todos os cabos existentes, inclusive os cabos de força; e capturar todos os dados voláteis que achar necessário.

Tem sido comum o uso da “Ata Notarial” para fins de prova legal em ambientes eletrônicos. Ela consiste em um instrumento público no qual o tabelião ou preposto autorizado, a pedido de pessoa capaz ou representante legal, materializa fielmente em forma narrativa o estado dos fatos e das coisas, de tudo aquilo que verifica com seus próprios sentidos sem emissão de opinião, juízo de valor ou conclusão, portando por fé que tudo aquilo presenciado e relatado representa a verdade¹⁶⁹, consignando em seu livro de notas, como previsto pela Lei federal n. 8.935/94. Alguns exemplos de situação em que ela se aplica é: a) para relatar *sites* invadidos; b) páginas para fraudes; c) *e-mails*; d) outros crimes que merecem ser relatados.

As situações mais comuns de análise forense nas empresas têm sido¹⁷⁰:

- *Análise de e-mails* — consiste na análise do teor de um *e-mail*, texto, *links*, imagens e informações de cabeçalho, que permite descobrir, entre outras informações, qual a máquina responsável pelo envio da mensagem, o servidor e o domínio utilizados para armazenar as imagens e/ou códigos maliciosos que a mensagem tenta instalar. Esses dados podem ser suficientes para que a em-

168. Basicamente essa teoria dispõe sobre a problemática da prova ilícita por derivação — aquela prova obtida de forma lícita, à qual, entretanto, se chegou por meio da informação extraída de prova ilícitamente colhida.

169. http://www.rcj.com.br/indice_colaboracoes.php?page=1 (Acesso em 21-7-2008).

170. Mais informações:

<http://www.guiatecnico.com.br/Periciaforense/> (Acesso em 21-7-2008).

presa possa impetrar as medidas judiciais cabíveis, a fim de que seja interrompida a fraude e até mesmo localizar o fraudador pelas vias judiciais.

- *Análise dos conteúdos Web* — o monitoramento e análise dos conteúdos dispostos na Internet para acesso irrestrito de usuários, considerado como o acesso obtido pelo usuário comum, desde que não exista a tentativa de desfigurar o *site* de forma não autorizada. Ou seja, é preciso que haja uma ordem judicial ou então um embasamento legal fundamentado no “direito de legítima defesa”. O uso de ataques do tipo DOS (Negação de Serviço) aos servidores, mesmo os que operem *sites* de renomados fraudadores, não é uma alternativa recomendável em termos de riscos legais.

- *Análise de conteúdos fechados para assinantes* — a mera observação dos conteúdos para tentar identificar os possíveis casos de fraude ou comprometimento de segurança não oferece riscos (monitoramento passivo). Sabemos, contudo, que muitos conteúdos só podem ser acessados por usuários “não anônimos” e que estejam “logados” no serviço, como é o caso dos fóruns de discussão, grupos de *e-mails*, *sites* de relacionamento (Orkut, entre outros) etc. Nesses casos deverão ser evitadas duas condutas, a saber: a) utilização de um cadastro particular/pessoal do funcionário; e b) criação de um cadastro falso.

- *Interação com os sujeitos objeto de monitoramento* — podem ser tentados os usos dos próprios meios dos *hackers* para tentar identificar e, assim, punir os fraudadores, com técnicas como engenharia social ou instalação de *trojans* nos equipamentos dos suspeitos. Tais práticas, contudo, podem ser entendidas como antiéticas e ilegais. A rigor, todo tipo de interação que se dê com os suspeitos objeto de monitoramento que não seja feita de forma institucionalizada deve ser evitada, e isso inclui todos os serviços de comunicação direta, telefone, *e-mail*, *Messenger*, *ICQ*, fóruns de mensagens e *sites* de relacionamento. Esse tipo de interação prejudica a validade das provas obtidas. Para ser feita do modo adequado é essencial obter uma ordem judicial, para que não se recaia em uma situação de “flagrante preparado”, “tocaia ilegal”, “falsa identidade”, entre outros. Há a forma certa de realizar esse tipo de atividade, que precisa ser por exceção e bem fundamentada.

Por fim, uma das principais questões que geram conflito na computação forense é a investigação *versus* o direito à privacidade. Até onde se pode ir sem violar a privacidade das pessoas envolvidas direta ou indiretamente no processo de perícia? Portanto, além de cautela, é necessário estar fundamentado nas leis que estão direta ou indiretamente relacionadas ao caso, evitando que de alguma forma a privacidade alheia seja violada, fazendo com que determinada perícia vá além dos limites de seu real objeto.

8.20. Leilão virtual

Uma das modalidades de negócios que mais crescem na rede é aquela que envolve o contato entre diferentes consumidores interessados em vender, trocar ou adquirir mercadorias e serviços. Essa prática é favorecida pela facilidade de oferecer determinado produto a um grande número de pessoas, como numa feira livre de grandes dimensões, sem ter de se deslocar fisicamente e sem ter de arcar com os custos de um anúncio nas sessões de classificados dos jornais.

Os *sites* que propõem tornar-se um ponto de encontro entre esses usuários são genericamente chamados de *sites* de leilão-virtual. Juridicamente, a definição não se aplica na maioria dos casos. Há uma grande diferença entre o Leilão Virtual e o Leilão Oficial *Online*¹⁷¹.

Segundo a legislação brasileira de leilões, a figura do leiloeiro é aquela que dá a referência do produto leiloadado, avalizando sua origem, qualidade e autenticidade¹⁷². Por ser o avalista do que é vendido, o leiloeiro recebe uma comissão¹⁷³

171. O instituto do leilão está indissociavelmente ligado à figura do leiloeiro, tanto que não existe uma lei sequer sobre o leilão especificamente: o que o ordenamento regula é a atividade do leiloeiro. A lei veda que terceiro estranho à classe dos leiloeiros realize o pregão (Dec. n. 21.981/32, art. 19), salvo nos casos nela previstos (art. 45). Além disso, existem outras características típicas de leilão, que não se encontram na maioria dos *sites* de Leilão Virtual, como a publicidade em jornal, prevista no art. 38 do referido decreto, e a proibição da realização de pregões em domingos e feriados, estipulada no parágrafo único do art. 36.

172. O Decreto n. 21.981, de 19 de outubro de 1932, Cap. III, que trata das funções dos leiloeiros em seu art. 21, *in fine*, determina que o leiloeiro deve proceder “na hipótese do comitente haver omitido os respectivos valores (das mercadorias móveis entregues à venda) a avaliação que julgar razoável, mediante comunicação que deverá ser entregue pelo protocolo ou por meio de carta registrada”.

173. Versam sobre a comissão do leiloeiro, entre outros, os arts. 22 e 24 do Decreto n. 21.981/32:

“Art. 22. Os leiloeiros, quando exercem o seu ofício dentro de suas casas e fora delas, não se achando presentes os donos dos efeitos que tiverem de ser vendidos, serão reputados verdadeiros consignatários ou mandatários, competindo-lhes nesta qualidade:

(...)

f) exigir dos comitentes uma comissão pelo seu trabalho, de conformidade com o que dispõe este Regulamento, e a indenização da importância despendida no desempenho de suas funções, acrescida de juros legais, pelo tempo que demorar o seu reembolso, e, quando os efeitos a ser vendidos ficarem em depósito litigioso, por determinação judicial, as comissões devidas e o aluguel da parte do armazém que os mesmos ocuparem, calculado na proporção da área geral e do preço de aluguel pago por este armazém.

(...)

Art. 24. A taxa de comissão dos leiloeiros será regulada por convenção escrita que, sobre todos ou alguns dos efeitos a vender, eles estabelecerem com os comitentes. Em falta de estipulação prévia, regulará a taxa de 5%, sobre móveis, mercadorias, joias e outros efeitos e a de 3%, sobre bens imóveis de qualquer natureza.

sobre o preço final do produto. Por isso, ele também é o responsável por valorizá-lo aos olhos dos possíveis compradores — em outras palavras, por “fazer o *marketing*” do produto em questão — e deve ser uma figura confiável perante os seus interlocutores. O leiloeiro que vende um produto desqualificado, que ludibria os consumidores, que passa informações erradas sobre o produto é um leiloeiro falido¹⁷⁴.

Essas características não são encontradas nos chamados *sites* de leilão virtual. Assim como eles não preenchem um dos requisitos básicos para que sejam considerados um leilão oficial: a publicação de editais com prazo de antecedência mínima, em todas as praças em que o leilão for ocorrer. Considerando a Internet, a opção seria a execução através de um veículo de mídia nacional, com cobertura sobre todo o território, ou por um edital *online* publicado na Internet nos locais de maior acesso de usuários, sendo que um não restringe o outro.

Feitas essas considerações, podemos apresentar o Leilão Virtual com algumas características distintas, dependendo de como é feita a oferta, a compra e de quem é a responsabilidade pela origem da mercadoria e pela entrega. Podendo ser: 1) Preço Mínimo/Maior Oferta; 2) Sem Preço Mínimo/Maior Oferta; 3) Oferta pelo Comprador; 4) B2B (*Business to Business*); 5) C2C (*Consumer to consumer*).

Um dos formatos mais populares é o de Preço Mínimo/Maior Oferta, modalidade mais próxima do conceito jurídico de leilão. O problema é que essa atividade é realizada sem a presença do leiloeiro, já que o vendedor e o potencial comprador interagem diretamente através da interface de comunicação do *site*. Alguns *sites* cobram comissão por disponibilizar essa interface; outros preferem lucrar apenas com o volume de visitas de suas páginas, tirando seu faturamento de eventuais anunciantes. Neste último caso, o *site* se assemelha mais a uma vitrina de anúncios classificados, não pesando sobre a empresa nenhuma responsabilidade quanto à qualidade dos produtos transacionados¹⁷⁵.

Parágrafo único. Os compradores pagarão obrigatoriamente 5% sobre quaisquer bens arrematados”.

174. Os leiloeiros são agentes auxiliares do comércio oficiais e, como tais, desfrutam seus documentos de fé pública, portanto é exigida do leiloeiro a maior retidão e transparência em suas atividades; se este proceder com dolo ou má-fé, além de responder civilmente pelos prejuízos que causar, poderá sofrer processo administrativo pela respectiva Junta Comercial, podendo em virtude deste ser punido com a suspensão ou até destituição do cargo de leiloeiro.

175. Se o *site* de fato age como uma “vitrina virtual”, veiculando apenas anúncios, a responsabilidade sobre estes recai em quem os fizer veicular de acordo com o art. 30 do Código de

O primeiro caso é mais complicado: se o *site* cobra comissão, age como um leiloeiro — nesse caso, teria, em princípio, que avaliar todos os produtos negociados (o que, devido ao volume gerado pela Internet, é bastante complicado). Se um consumidor for lesado num *site* desse tipo, o ônus de compensá-lo deve ficar com a empresa que fez a intermediação, no caso, o *site*¹⁷⁶. Isso obrigará os *sites* que quiserem cobrar comissões a conhecer as mercadorias negociadas, trazendo credibilidade para o próprio *site*, pois o consumidor se sentirá seguro quando realizar uma compra. No primeiro caso, a empresa pode até cobrar pelo serviço (como um jornal cobra pelos anúncios sem ter a obrigação de garantir a autenticidade do que é anunciado); mas é importante que a cobrança não se estenda a uma comissão sobre o valor de venda. É muito melhor que o *site* se caracterize como um *e-market*, uma feira livre virtual de troca de mercadorias, do que como um *site* de leilão, em razão do nível de responsabilidade jurídica que sobre este último recai.

É importante destacar que se o *site* de leilão deixa claro os mecanismos de segurança e os mesmos não são seguidos pelos usuários (comprador ou vendedor), em situação de eventual incidente a justiça tem entendido pela aplicação do art. 14, § 3º, do Código de Defesa do Consumidor, que exime de responsabilidade um fornecedor de um serviço se ficar provada a culpa exclusiva do cliente¹⁷⁷.

Defesa do Consumidor.

176. "EMENTA: MEDIDA CAUTELAR — Abstenção de veiculação de anúncio de venda de produtos da marca 'Diesel' pela Internet, sob pena de multa diária — Liminar concedida — Ordem mantida — Pleito que encontra lastro em contrato de distribuição exclusiva de produtos importados — Oferta em *site* de comércio eletrônico de mercadorias contrafeitas com essa marca, ou originais ilegalmente adentradas no país — Atividade deste, que embora lícita, contribui para a prática desses ilícitos, com os quais auferem vantagem econômica (...)" (TJSP, rel. Des. Galdino Toledo Júnior, AgI 448.555-4/4, j. 22-5-2007).

177. "EMENTA: Responsabilidade Civil. Ação de reparação por danos morais e materiais (...). Obrigação de indenizar não reconhecida. Conjunto probatório dos autos que aponta ter havido culpa exclusiva da vítima, ao não observar os procedimentos de segurança oferecidos no *site* da empresa-ré, no intuito de garantir a entrega da mercadoria pelo vendedor e o pagamento do valor pelo comprador, tendo optado por transacionar diretamente com o pretense comprador e confiar no *e-mail* fraudulento enviado por este, desconsiderando por completo o aviso remetido pela apelada (...)" (TJRJ, rel. Des. Maria Inês da Penha Gaspar, Ap. 2008.001.16030, j. 9-4-2008).

"Ação de reparação de danos. Compra e venda de bem móvel por meio da internet. Sentença devidamente fundamentada, com clara exposição das razões de decidir. Inexistência de afronta ao mandamento contido no art. 93, IX, da Constituição Federal. Elementos de prova suficientes para a formação da convicção. Julgamento antecipado que não configura cerceamento de defesa e, ao revés, consagra o princípio da razoável duração do processo. Compreensão do art. 330, I, do CPC. Empresa que se insere no mercado de prestação de serviço, disponibilizan-

Outro formato é o de Sem Preço Mínimo/Maior Oferta, modalidade que foge um pouco do conceito tradicional de leilão e tem sido comumente utilizada para a oferta de produtos diferenciados ou exclusivos, como uma coleção de discos raros, uma peça de arte ou uma mobília antiga. Se pensarmos que para que qualquer ato seja caracterizado como um ato de compra e venda, basta que haja ajuste de preço, forma de pagamento e entrega, temos aqui, por

do *site* na internet para, mediante remuneração, facilitar negócios, não está imune às intercorrências advindas. Formação da obrigação de suportar, solidariamente com aquele que violou direito, o prejuízo causado ao consumidor. Ausência de cautela básica, que de todo se exige, que estabelece a culpa concorrente do consumidor. Dano moral somente se forma quando há violação ao direito de outrem, sem que para tanto este concorra para o resultado. Desídia consistente que veda a imposição de indenização por danos morais. Recurso do corréu desprovido. Recurso do autor parcialmente provido" (TJSP, Apelação 9209343-73.2006.8.26.0000, rel. Des. Dimas Rubens Fonseca, j. 11-10-2011).

"Apelação cível. Responsabilidade civil. Provedor de internet. Mercado Livre. Opção pela modalidade "Mercado Pago". Mensagem eletrônica (*e-mail*) enviado por terceiro fraudador como se fosse o provedor prestador do serviço. Risco intrínseco à atividade que configura fortuito interno, ensejando a responsabilidade do fornecedor de serviços. Dever de informar o risco não satisfatoriamente cumprido. Ausência de dano moral. O risco de um terceiro obter as informações e enviar mensagem eletrônica como se fosse o provedor deveria ser claramente advertido, assim como a imposição de que o consumidor-vendedor verifique no *site* sua conta antes de remeter o produto. Não pode o fornecedor de serviços se utilizar de fontes grandes e claras em cores chamativas no seu *site* para alardear as qualidades de seu produto e deixar as informações sobre os riscos e medidas de segurança para serem explicitadas apenas no contrato de adesão. Se a informação não foi comprovadamente fornecida de maneira adequada ao consumidor — ônus que incumbe ao fornecedor — o risco da atuação fraudulenta de terceiro deve recair sobre o fornecedor, o qual deve responder perante o consumidor e buscar o terceiro em ação regressiva. Fato ensejador de dano patrimonial, pelo envio da mercadoria sem recebimento do preço prometido, mas não de dano moral. Recurso a que se dá parcial provimento" (TJRJ, Apelação Cível 0200216-28.2007.8.19.0001, rel. Des. Marcia Ferreira Alvarenga, j. 13-4-2011).

"Apelação. Ônus da prova. Contrato de prestação de serviços. Venda de produtos pelo *site*. Ausência de prova da contratação. Teoria do risco proveito. Dano moral. Configurado. *Quantum*. Proporcionalidade. O ônus de provar a celebração do negócio jurídico é do réu, já que é impossível ao requerente provar que não efetuou o anúncio no *site* réu. A referida prova é tida pela doutrina como prova diabólica, já que trata de uma prova negativa no qual é impossível a sua produção. O sistema de contratação dos anúncios via internet é frágil, já que possibilita a fraude de terceiros. A culpa da empresa ré está configurada pelo fato de disponibilizar um sistema frágil de contratação que coloca em risco o direito de outrem. Trata-se da teoria do risco proveito prevista no art. 927, parágrafo único, do Código Civil. Se o sistema disponibilizado falhou, a empresa de ré deve arcar com os prejuízos causados a parte, principalmente considerando que a mesma lucra pela venda realizada. Os danos morais estão configurados, já que o autor foi acusado de vender um aparelho celular e não entregá-lo, fato este que denegriu a honra do requerente. O valor da reparação por danos morais visa recompor o abalo sofrido. Deve ser arbitrado com proporcionalidade, tendo em vista a extensão do dano e as condições econômicas do violador do dever de cuidado" (TJMG, Apelação Cível 1.0625.10.000297-5/001, rel. Des. Ti-búrcio Marques, j. 17-2-2011).

analogia, na verdade, o modelo jurídico do contrato de compra e venda¹⁷⁸. Mais uma vez, se houver cobrança de comissão pelo *site*, este assume certas responsabilidades perante o bom andamento da negociação — as mesmas responsabilidades jurídicas de um corretor¹⁷⁹.

Há ainda o tipo com Oferta pelo comprador, mais conhecido como Leilão Reverso. Essa modalidade foge totalmente às regras do leilão tradicional, já que os vendedores passam a disputar o preço do comprador. É muito semelhante a um pregão — o desejo de compra passa a ser negociado como uma *commodity*.

Outra modalidade, feita apenas entre empresas, é conhecida como Leilão B2B (*business to business*), usada principalmente para a venda de estoques de mercadorias entre empresas. Aqui não se aplica o Código de Defesa do Consumidor.

Finalmente, há a modalidade realizada diretamente entre consumidores nas duas pontas, que é o Leilão C2C (*consumer to consumer*), em que o *site* de leilão não se responsabiliza nem pelo produto vendido, nem pela entrega dele. É apenas um espaço para a transação entre os consumidores. Nesse caso, mais uma vez, pesam sobre o *site* as responsabilidades previstas no caso de cobrança de comissão.

É importante ressaltar que, quando o estoque é próprio, ou, como se costuma chamar normalmente, *inhouse*, o *site* de leilão passa a ser considerado, legalmente, como um revendedor, com todas as responsabilidades legais¹⁸⁰ que esse *status* lhe confere.

Em todos os casos, a maioria das vendas é feita fora do estabelecimento do fornecedor, o que não impede que seja aplicado o art. 49 do Código de Defesa do Consumidor, que prevê a possibilidade de o consumidor desistir do

178. Assim se depreende das normas que regulam o instituto, art. 481 do Código Civil: “Pelo contrato de compra e venda, um dos contratantes se obriga a transferir o domínio de certa coisa, e o outro, a pagar-lhe certo preço em dinheiro”.

179. Notamos que, da maneira como se apresentam atualmente os *sites* de leilão virtual, é difícil caracterizar seus serviços como de leilão, devido às restrições legais. Por outro lado esses serviços assemelham-se muito à mediação realizada pelo corretor. Aos corretores, desde a antiga Roma, atribui-se a função de aproximação das partes interessadas em negociar. Acreditamos que por analogia as responsabilidades de um *site* de leilão virtual são equiparáveis às do corretor livre, podendo ser ampliadas nos casos em que o *site* possui a guarda da coisa a ser vendida, respondendo então perante o consumidor pelos possíveis defeitos da coisa, bem como por seus vícios ocultos.

180. Ao se caracterizar como revendedor, o *site* acaba por assumir uma responsabilidade objetiva em face dos consumidores e se submete totalmente ao Código de Defesa do Consumidor.

contrato no prazo de sete dias contados do recebimento do produto ou serviço, em se tratando, é claro, de consumidor final.

É importante, por último, ressaltar que os *sites* devem preocupar-se em disponibilizar contratos para os usuários em que esteja incluída a opção de cláusula de arbitragem. Nesses casos, o consumidor terá uma garantia a mais da segurança da operação, já que poderá ter a alternativa de resolver o conflito amigavelmente, o que sem dúvida agrega um enorme valor ao próprio *site*.

8.21. Pregão eletrônico

O pregão, em princípio, é uma modalidade de licitação, regulada pela Lei n. 10.520/2002. O seu advento se deve ao poder do legislador federal em criar nova modalidade de licitação, conforme previsto pelo § 8º do art. 22 da Lei n. 8.666/93.

Desse modo, com o crescimento do uso da Internet e das ferramentas de comunicação, o pregão ganhou uma versão eletrônica. Sua maior diferença para a versão presencial (física) está no fato de a sessão pública e os atos pertinentes ao mesmo serem realizados todos por meio de sistema eletrônico, via Internet¹⁸¹.

Desde então, o pregão passou a ser amplamente utilizado por ser um processo mais célere. Em termos legais, sua aplicação deve destinar-se à aquisição de bens e serviços comuns, segundo o Decreto n. 5.450/2005, ou seja, aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos no edital, por meio de especificações usuais do mercado. É importante destacar que deve haver rigidez no cumprimento do princípio da igualdade, visto que em um processo licitatório não pode haver procedimento seletivo com discriminação entre participantes ou cláusulas que afastem eventuais proponentes qualificados ou, ainda, que favoreça uns ou prejudique outros no julgamento.

As mesmas regras básicas do pregão presencial, tais como modalidade, disputa etc., aplicam-se ao pregão eletrônico. O seu formato virtual tem como vantagens permitir o uso de novas tecnologias da informação, garantir maior acesso e participação ao pregão, atendendo ao princípio da igualdade, visto que reduz, inclusive, barreiras geográficas (uma empresa de outra cidade consegue

181. Para saber mais sobre pregão eletrônico: “Pregão Eletrônico: a mais moderna modalidade de licitação”, 2. ed., 2005, Editora Temas e Ideias, do autor Sidney Bittencourt. Ver também *websites* <www.governoeletronico.gov.br>, <http://www.siapre.com.br/conteudo/siapre_inform.html> e <www.aceessa.com/informatica/arquivo/tecnologias/2002/06/07-pregao>.

participar facilmente da quotação), dá maior agilidade para todo o processo, transparência e, por tudo isso, economia.

O critério de julgamento é o menor preço¹⁸², no entanto, deve-se destacar que se o bem não for comum, ou se sua contratação exigir outro critério de julgamento, como técnica e preço, não deve ser usado o pregão eletrônico.

O pregão eletrônico veio para ficar, mas ainda deve ser melhorado no sentido de garantia de autoria das propostas, para evitar manipulação de preços. Por isso, há discussão sobre a exigência de uso de algum tipo de “identidade digital”, tal como uma assinatura ou certificado da ICP-Brasil, mas este requisito fere o princípio do livre acesso e participação. Outras questões envolvendo segurança da informação também têm sido levantadas, principalmente para proteção do ambiente de dados da plataforma usada para o pregão, o que cabe ao ente público administrar.

8.22. Finanças virtuais e o Internet Banking

Como vimos, o mundo das transações eletrônicas tem sua origem nas empresas financeiras. Bancos e corretoras de valores operam eletronicamente processando informações, compensando cheques, créditos e débitos, efetuando negócios há muito tempo. Há outros princípios importantes para se pensar a partir do momento em que esse mundo é transposto para o universo da Internet, chegando a um número cada vez maior de pessoas: os princípios de segurança, solidez e credibilidade, tão velhos como as próprias instituições financeiras. Não há como falar de agência bancária sem associar com “segurança”, com “proteção e guarda de dinheiro e/ou outros bens”.

Para nós está claro que no mundo virtual as instituições bancárias têm de ter a mesma segurança, solidez e credibilidade perante os seus clientes que no mundo real — ou até mais, pelas características da rede. O custo de uma operação bancária feita na agência é superior ao daquela feita por telefone, e este é, por sua vez, superior ao da feita pela Internet. Por este motivo, é estratégico que os clientes da era digital “não precisem ir na agência”. A credibilidade do uso dos recursos de tecnologia da informação no mercado financeiro é fator crucial para sua própria viabilidade atual.

182. Devemos destacar que para a contratação de bens e serviços de informática a Administração adotará obrigatoriamente o tipo de licitação “técnica e preço”, permitido o emprego de outro tipo de licitação nos casos indicados em decreto do Poder Executivo (§ 4º do art. 45 da Lei n. 8.666/93).

Mas a partir do momento em que as relações entre correntistas e bancos migraram para o ambiente virtual, passou-se a ter maior dificuldade em se delimitar um perímetro de responsabilidade, que até então era definido claramente por barreiras físicas (“a porta da agência”, “o cofre”).

Por este motivo que cada vez mais se discute sobre quais os limites da responsabilidade do Banco e quais são as obrigações de segurança que o cliente deve tomar para evitar riscos.

É claro que o ambiente do *website* do Banco é responsabilidade deste. Um roubo virtual sofrido por um cliente quando operava no *site* de um banco é de responsabilidade desse banco¹⁸³. Assim como também deveria ser nítida a responsabilidade do cliente pelo nível de segurança de seu equipamento (computador, celular, outro tipo de *handheld*), e de sua conexão à Internet para acessar o Banco. No entanto, a Justiça brasileira ainda não tem um posicionamento bem consolidado.

Já em se tratando de Mercado de Risco, como a Bolsa de Valores, o Mercado Financeiro Virtual tem afinidades com o Mercado Financeiro Real e ao mesmo tempo distinções. A afinidade é que são ambos baseados em comunicação eletrônica de dados e informação. A principal diferença é a qualidade do usuário. Isso quer dizer que o participante do mercado virtual é normalmente muito mais amador do que o do mercado real, até por uma questão de acessibilidade, que possibilita a pessoas que nunca investiram na bolsa resolver tentar a sorte. Essa peculiaridade exige que os requisitos que a Comissão de Valores Mobiliários já impõe ao mercado real sejam cuidadosamente observados e até mesmo aumentados para a prática no mercado virtual.

As principais regras de conduta adotadas no Mercado Financeiro Real, de acordo com o art. 3º da Instrução CVM n. 387/2003, são: a) proibidade na condução das atividades; b) zelo pela integridade do mercado, inclusive quanto à seleção de clientes e à exigência de depósito de garantias; c) diligência no cumprimento de ordens e na especificação de comitentes; d) diligência no controle das posições dos clientes na custódia, com a conciliação periódica entre: ordens executadas, posições constantes em extratos e demonstrativos de movimentação fornecidos pela entidade prestadora de serviços de custódia, posições fornecidas pelas câmaras de compensação e de liquidação; e) capacitação para desempenho das atividades; f) obrigação de obter e apresentar a seus clientes informações necessárias ao cumprimento de ordens, inclusive sobre

183. Ver Lei n. 7.102/83 que revogou os Decretos ns. 1.031/69 e 1.103/74.

riscos envolvidos nas operações do mercado; g) adoção de providências no sentido de evitar a realização de operações em situação de conflito de interesses e assegurar tratamento equitativo a seus clientes; h) suprir seus clientes, em tempo hábil, com a documentação dos negócios realizados.

Outros pontos também merecem destaque, conforme previsto no art. 5º da Instrução CVM n. 387/2003¹⁸⁴: as corretoras devem manter registro de todas as movimentações financeiras de seus clientes em contas correntes não movimentáveis por cheques, bem como devem cadastrar seus clientes e manter os cadastros atualizados, junto às bolsas, câmaras de compensação e liquidação e às entidades prestadoras de serviços de escrituração e custódia, permitindo a perfeita identificação e qualificação deles.

A estes princípios devem-se somar outros para que o Mercado Financeiro Virtual seja um ambiente sadio e seguro para realização de negócios: a) obrigatoriedade de a corretora *online* dar cursos de instrução para capacitação de investidores virtuais; b) transparência na divulgação de informações; c) divulgação clara do tempo que leva para a operação virtual ser efetivamente concluída; d) notificação por escrito do cliente a respeito das regras da corretora sobre recebimento, registro, prazo de validade, prioridade de execução, distribuição e cancelamento de ordens virtuais.

É importante observar que na Internet é mais fácil não apenas disseminar informação como também lhes dar uma aparência de procedência confiável, mas que, na verdade, muitas vezes não é verificada¹⁸⁵. A responsabilidade maior por tal checagem é da corretora, que tem o dever de prestar posterior informação¹⁸⁶ a seus clientes. Nesse sentido, os agentes têm a obrigação de verificar se as informações disponíveis na Internet sobre ações, recomendações de compra ou venda, entre outras, são verdadeiras.

184. A Instrução CVM n. 505/2011 revogou a Instrução CVM n. 387/2003, que por sua vez revogou toda a Instrução CVM n. 382/2003, que regia esta matéria anteriormente.

185. Pode incorrer em pena de detenção e multa, nos termos do art. 16, II, da Lei n. 5.250/67 (Lei de Imprensa), aquele que publicar ou divulgar notícias falsas ou fatos verdadeiros truncados ou deturpados, que provoquem desconfiância no sistema bancário ou abalo de crédito de instituição financeira ou de qualquer empresa física ou jurídica.

186. O dever de prestar informação da corretora é um dos princípios exigidos pela CVM, na relação desta com seus clientes, no inciso VI do art. 3º da Instrução CVM n. 387/03: "*Art. 1º As bolsas devem estabelecer regras de conduta a serem observadas pelas corretoras no relacionamento com seus clientes e com os demais participantes do mercado, atendendo aos seguintes princípios: (...) VI — obrigação de obter e apresentar a seus clientes informações necessárias ao cumprimento de ordens, inclusive sobre riscos envolvidos nas operações do mercado*".

Em virtude da fluidez e da velocidade da informação na Internet, o meio virtual exige uma fiscalização diferenciada¹⁸⁷ das corretoras que operam apenas virtualmente ou que praticam operações de *day-trade*, pois o sistema *online* permite que se disseminem rapidamente boatos, e o volume de operações simultâneas em cadeia pode colocar em risco até investidores mais experientes.

Um dos maiores desafios jurídicos dos últimos anos tem sido desenvolver tecnologias que possam viabilizar a manifestação de vontade não presencial com menor risco possível. Sendo possível obrigar-se juridicamente independente de "espaço-tempo" dentro do princípio da presunção da boa-fé contratual. Desse modo, hoje vivemos em uma "Era Digital", em que tudo é documentado nas relações que ocorrem em sua maior parte pela via eletrônica, e com menos geração de papel. O meio digital permite inclusive o efeito da "simultaneidade", que favorece a celebração de acordos, votações, eleições. Melhor do que quando há necessidade de tempo diferido (modelo carta, *e-mail*, outros).

A assembleia *online* já é uma realidade. Para entender seu funcionamento, inclusive sob a ótica das Sociedades Anônimas (S.A.), precisamos compreender que o ponto principal da questão está em como conseguir determinar autenticidade de emissão e uso da outorga de poderes (evidências de autoria e integridade) mais do que o formato ou o suporte que poderá receber. Para o Direito, é relevante saber que as partes tinham intenção de se fazer representar, qual a qualificação ou dados de ambos (outorgante e outorgado) e sua data (validade). Deve-se atender à exigência do art. 126 da Lei das S.A., e sempre vislumbrar a igualdade de condições entre os acionistas. Estes são os requisitos jurídicos essenciais. Outros elementos técnicos que se possa adicionar para evitar "má-fé" são desejáveis, mas não indispensáveis.

A assinatura com base no certificado digital emitido pela ICP-Brasil equipara à assinatura com firma reconhecida, válida no Brasil. Isso vai além do requisito legal para a Assembleia de Acionistas em vigor (nem o Código Civil nem a Lei das S.A. exigem o reconhecimento de firma ou a consularização das procurações, até para evitar qualquer tipo de discriminação entre eles). Assim, a companhia sempre poderá, a seu critério, dispensar o reconhecimento de firma e a consularização dos instrumentos de procuração outorgados pelos acionistas a seus representantes. Até porque a Assembleia é uma reunião privada, cabendo à companhia determinar o modelo de autenticação que irá aceitar e que seja válida e aplicável a todos igualmente. O que também está

187. Ver Instrução CVM n. 438/2006, que revogou a Instrução CVM n. 365.

previsto pela própria MP 2.200-2/01, em seu art. 10, § 2º, deixa claro que podem ser usados certificados digitais não emitidos pela ICP-Brasil, desde que observada a admissão de sua validade entre os acionistas e a Companhia, com critérios e regras previamente estabelecidos.

Concluimos que é possível estabelecer de forma prévia, clara, igualitária um modelo de Assembleia *Online* de Acionistas, formalizada pela Política de Participação em Assembleia, que deve ser comunicada a todos. O mecanismo de verificação da outorga de poderes deve ser idôneo, o que pode ser feito inclusive por meio de um sistema, como via Internet Banking (em que há um operador *master* e um operador subordinado, com uso de *login*, senha, *token*). Não necessariamente precisa ser feito uso de Certificado Digital ou mesmo da ICP-Brasil. Deve-se ter cuidado para usar um recurso que permita participação ampla de todos, de qualquer lugar. Exigir que seja usado certificado digital da ICP-Brasil seria na verdade um elemento impeditivo, em especial para acionistas estrangeiros ou residentes em outros países.

Qualquer forma de participação *online* sempre terá o desafio de verificar autoria, que a pessoa que está do outro lado da tela seja ela mesma. Nesse ponto, qualquer um pode estar de posse de um certificado digital da ICP-Brasil e saber a senha. Isso não vai impedir que uma pessoa se passe por outra (somente o método biométrico tem esse nível de eficácia jurídica). A TI tem que estar sempre alinhada ao negócio! Não há riscos legais novos sem migrar o modelo de Assembleia de Acionistas para o formato *online*, ao contrário, estar-se-ia viabilizando o princípio da ampla participação em igualdade de condições.

No caso das corretoras, a Internet traz uma nova dimensão ao mercado de capitais: as *home brokers*¹⁸⁸, corretoras que dão ao usuário comum a possibilidade de participar diretamente¹⁸⁹ do mercado de compra e venda de ações e

188. "Home broker é o sistema pelo qual os investidores, através de corretoras que possuem programa de computador específico que permite a conexão ao sistema 'Mega Bolsa' da Bolsa de Valores de São Paulo, negociam valores mobiliários através do envio direto de ordens de compra e venda de seus próprios computadores, sem a participação do operador" (Eduardo, Patrícia Fischer de Paula. Internet e Mercado de Valores Mobiliários. In: *Internet — O direito na era virtual*).

189. Isso é possível graças ao sistema de "ordens", atos pelos quais os investidores determinam à corretora a compra ou venda de valores mobiliários ou direitos a eles inerentes em seu nome e nas condições que especificar. Então, através dos vários tipos de ordens aceitos pelas Corretoras de Valores, pode o usuário determinar não só a quantidade e as características dos valores mobiliários, como também uma série de outras variantes, por exemplo, o prazo de validade das ordens de operações. No caso de a ordem não ser efetivada no mesmo dia, ela pode, se assim estipulado, ser válida para o dia seguinte nas condições que o cliente estabelecer, como a cláusula de não execução no caso de alta dos preços.

títulos. Essas empresas aumentam bastante o potencial especulativo do mercado acionário: boatos lançados em um meio repleto de usuários despreparados para as nuances do setor podem ter consequências drásticas para determinadas ações — e para a economia como um todo. Além disso, os *home brokers* costumam, irresponsavelmente, vender a ideia de que os investimentos em ações são uma maneira fácil de ganhar dinheiro, sem alertar suficientemente os usuários comuns sobre os grandes riscos inerentes a esse mercado. Uma maneira de solucionar o problema seria obrigar os *home brokers* a credenciar os usuários, fazendo-os inclusive passar por uma fase de testes¹⁹⁰, o que os faria acostumar a operar na Bolsa e aprender sobre os riscos e macetes da operação, recebendo um certificado eletrônico, ao fim de determinado período, que os habilitaria às operações. É importante que consultores especializados estejam disponíveis, durante essas operações, para atender a dúvidas e questionamentos dos usuários, não os deixando simplesmente entregues a um mundo que não conhecem bem.

8.23. Aspectos legais do Home Broker

Em 1999 o Conselho de Administração da BOVESPA¹⁹¹ criou o programa *Home Broker*, cuja finalidade era enviar recursos financeiros, técnicos e humanos para sociedades corretoras membros com a intenção de criar em suas sedes sistemas automatizados, baseados na concepção e na tecnologia existente naquela época para que tais sistemas fossem hospedados em *websites* seguros.

O uso desses *websites* seguros permitiram um relacionamento automatizado entre o cliente-investidor e as corretoras. Assim, o cliente teria acesso à sua carteira, cotações e análises sobre o mercado financeiro e de capitais e ainda poderia, sem nenhum contato com a mesa de operações, mas sob o controle desta, requerer a compra ou venda de ações para execução imediata ou programada no sistema eletrônico da BOVESPA, também conhecido como Mega Bolsa.

Sendo assim, podemos entender o *Home Broker*, conforme informações da própria BOVESPA, como um instrumento que permite a negociação de

190. Algumas corretoras que operam exclusivamente por meio eletrônico disponibilizam aos seus usuários simuladores de mercado em que os investidores iniciantes podem adquirir experiência e contar com a assessoria de profissionais para responder as possíveis dúvidas surgidas. O jornal *Folha de S. Paulo* disponibiliza um simulador (<http://folhainvest.folha.com.br/>) e incentiva com prêmios para os melhores colocados na participação e uso da ferramenta.

191. Fonte: <<http://www.infomoney.com.br>>, artigo de autoria de Gabriel Casonato de julho de 2008. Ver <http://pt.wikipedia.org/wiki/Home_Broker> e <http://www.empresario.com.br/bolsa/on_line/on_line.html>.

ações via Internet¹⁹². Ele permite que o investidor envie ordens de compra e venda de ações por intermédio do *site* de sua corretora na Internet, sendo requisito da operação via Internet que o investidor seja cliente de uma Corretora da BOVESPA que disponha do sistema *Home Broker*.

De forma similar aos serviços dos Bancos conhecidos como *Home Banking*, os *Home Brokers* das Corretoras são interligados ao sistema de negociação da BOVESPA¹⁹³ e oferecem vantagens como: agilidade no cadastramento e no trâmite de documentos; acompanhamento em tempo real da carteira de ações; acesso às cotações (algumas corretoras poderão oferecer também notícias e análises sobre o mercado); envio de ordens imediatas, ou programadas, de compra e venda de ações; recebimento da confirmação de ordens executadas etc.

No entanto, uma vez que o *Home Broker* cria um facilitador de entrada de investidores no mercado, muitos pela primeira vez, já que incentiva certa "autogestão", há alguns riscos que devem ser observados, tais como: riscos inerentes ao Mercado de Ações; riscos operacionais do uso da Internet; e riscos relacionados ao ciclo de liquidação.

Entre esses riscos expostos, o que mais gera impactos jurídicos, considerando esse novo modelo, vem a ser o risco operacional do uso da Internet e a responsabilidade das corretoras alusiva à segurança da informação.

O serviço de *Home Broker* possui regulamentação própria e exige prévia autorização da BOVESPA, bem como o cumprimento de alguns requisitos pelas Corretoras. Cabe a cada parte na operação (BOVESPA, Corretora, Cliente) cuidar da segurança do seu ambiente.

No tocante à criação do *website* que apresentará os serviços de *Home Broker* para os investidores, a Corretora deve observar as seguintes regras: a) o nome da Corretora deve sempre aparecer com destaque em todas as páginas do *website*, campanhas publicitárias, folhetos, entre outros veículos de comunicação; b) o nome da Corretora deve preceder a marca de fantasia com o mesmo peso gráfico; c) o Selo BOVESPA é obrigatório em todas as páginas do *website* relacionadas com o *Home Broker*; d) a Corretora deve informar no *website* se as cotações são fornecidas em tempo real ou com atraso de quinze minutos; e) outras instituições que têm acesso ao *Home Broker* (exemplos Distribuidoras de Títulos e Valores Mobiliários) devem informar nos respectivos *websites* que

192. Fonte: <<http://www.bovespa.com.br/Mercado/RendaVariavel/Homebroker/Homebroker.asp>>.

193. Fonte: <<http://www.bovespa.com.br/Bovespa/Tecnologia.htm>>.

não executam diretamente as ordens recebidas de seus clientes, identificando a Corretora que irá cumpri-las.

O serviço de *Home Broker* era regido pela Instrução CVM n. 376, que foi revogada e substituída pela Instrução CVM n. 380, art. 22.

Cabe à Corretora a responsabilidade pela segurança dos sistemas bem como pelo sigilo de toda a informação de seus clientes, devendo, para tanto, utilizar elevados padrões tecnológicos de segurança de rede, sendo as corretoras responsáveis também pela operacionalidade de seus sistemas, ainda que eles sejam mantidos por terceiros.

Tendo em vista que a operação ocorre eletronicamente, e inclusive com documentação de ordens de compra e venda por *e-mail*, deve a corretora guardar tal documentação por pelo menos cinco anos, considerando as normas aplicáveis tanto relacionadas ao mercado financeiro como também ao Código Civil e ao Código de Defesa do Consumidor.

Para evitar riscos no uso do serviço de *Home Broker*, é recomendável que a Corretora disponibilize conteúdo orientativo e de educação dos investidores, bem como elabore um "Termo de Uso" detalhado.

Em termos jurídicos, para proteção da própria Corretora, deve ficar claro quais são as obrigações do usuário, tais como: a) fazer uso de acesso seguro à Internet; b) criar uma senha forte (alfanumérica com caracteres especiais) e fazer a guarda segura dela e sua mudança periódica (pelo menos a cada 90 dias); c) possuir antivírus instalado no equipamento de acesso ao *Home Broker* e que deve estar sempre ativo e atualizado antes do acesso; d) nunca executar arquivos anexados por *e-mail* sem antes verificar a possibilidade de estarem contaminados por vírus; e) fazer a atualização do navegador (*browser*) para melhorias de segurança; f) evitar o uso de equipamento que não seja de sua confiança (especialmente equipamento público ou de uso coletivo, tal como cybercafé) e não utilizar aplicativos desconhecidos; g) acompanhar as movimentações de sua conta constantemente por meio de extratos periódicos e informar o operador imediatamente se houver qualquer crédito ou débito irregular.

Além das recomendações no que tange à segurança, é recomendável que o usuário de *Home Broker*, antes de firmar contrato com alguma corretora, verifique se ela cumpre os seguintes requisitos de informação em seu *website*, de forma clara, precisa e em linguagem acessível¹⁹⁴:

194. Conforme artigos da Instrução CVM n. 380.

— instruções detalhadas de uso do sistema de negociação de valores mobiliários pela Internet;

— os descontos praticados sobre suas tarifas para todos os clientes ou para classes específicas de clientes e os custos adicionais de negociação pela Internet, incluindo emolumentos cobrados por bolsa de valores ou entidade administradora de mercado de balcão organizado;

— os procedimentos detalhados seguidos pela corretora eletrônica na execução das ordens de compra e venda recebidas pela Internet, incluindo a possibilidade de as ordens não serem executadas automaticamente pelo sistema, e sua prioridade diante das ordens recebidas por outros canais de comunicação, segundo volume operado e outros parâmetros;

— as características do sistema de segurança mantido pela Corretora, incluindo uso de senhas e assinaturas eletrônicas;

— as formas eletrônicas utilizadas para comunicar ao investidor a recepção e fiel execução de suas ordens, bem como quaisquer outras informações que o investidor deva receber;

— informações sobre valores mobiliários, incluindo o melhor preço e as listas de ofertas, classificadas por valor mobiliário, vigentes nos sistemas de negociação eletrônica mantidos por bolsa de valores ou entidade administradora de mercado de balcão organizado, por meio do qual a corretora execute as ordens recebidas pela Internet, bem como o horário de divulgação dessas informações na página da Corretora na rede mundial de computadores;

— a corretora eletrônica responsável pela execução das ordens recebidas pela Internet, nos casos de repasse de ordens;

— o intervalo de tempo máximo sem realizar operações em que o investidor poderá permanecer conectado ao sistema de negociação pela Internet sem ser automaticamente desligado;

— atalho para página da CVM na Internet;

— exibir uma seção ou um atalho para a educação dos investidores com descrição da estrutura e do funcionamento das bolsas de valores, das entidades administradoras de mercado de balcão organizado e das câmaras de liquidação e custódia de valores mobiliários;

— informar sobre os riscos de oscilação de preço e eventuais perdas do valor principal inerentes ao mercado de valores mobiliários, particularmente aqueles decorrentes de posições em derivativos, os riscos operacionais do uso da Internet de sistemas eletrônicos de negociação para a compra e venda de valores mobiliários; os riscos decorrentes da falta de entrega de ativos no prazo

estipulado, bem como as medidas adotadas pelas câmaras de liquidação e custódia para reduzi-los;

— os procedimentos especiais de leilão, observadas as normas da CVM e bolsas de valores ou entidades administradoras de mercado de balcão organizado, às quais as ordens dos investidores estiverem sujeitas;

— informações relativas à competência das entidades autorreguladoras, principalmente no que se refere aos poderes para cancelar negócios previamente realizados, no caso de serem constatadas infrações aos dispositivos legais;

— informações sobre negociação simultânea de valor mobiliário na sala de pregão viva-voz e no sistema de negociação eletrônica, e quais os critérios de interferência de um mercado em outro; e

— ter em destaque o seguinte informe: “*Toda comunicação através da rede mundial de computadores está sujeita a interrupções, podendo invalidar ordens ou negociações*”.

Sendo tomadas as devidas precauções, tanto a Corretora como o Cliente-investidor estarão protegidos¹⁹⁵.

8.24. Mobile Banking e Social Banking

O presente capítulo é um estudo rápido sobre as principais questões técnicas e legais envolvendo o uso de *mobile banking* no Brasil, considerando a tendência internacional de criação do conceito de “agência móvel”. Tendo em vista o avanço do uso do *mobile banking* e com o crescimento das redes sociais, vimos necessidade em tratar sobre a participação dos bancos nas redes sociais como uma nova forma de se aproximar de seus clientes.

Já há bancos nacionais que disponibilizam esse tipo de plataforma, tais como o Banco do Brasil e o Bradesco, e o *benchmarking* internacional é o do Banco da Coreia. Há ainda o padrão europeu, bem como o incentivo do BACEN na adoção de padrões para uso de redes com mobilidade. Do ponto de vista jurídico, há uma série de requisitos que precisam ser preenchidos, de modo a garantir o cumprimento da legislação nacional, especialmente no tocante à geração de prova eletrônica, não repúdio, privacidade e segurança da informação. Já nas redes sociais, por sua vez, devem ter um canal oficial que tenha a

195. Para saber mais sobre *Home Broker* e que corretoras prestam este tipo de serviço, ver <<http://www.bovespa.com.br/mercado/rendavariavel/HomeBroker/FormConsultaHomebroker.asp>>.

característica informacional, de relacionamento ou de atendimento com o seu cliente.

Considerando a decisão do STF de 2006¹⁹⁶ que determina que os bancos estão sujeitos ao Código de Defesa do Consumidor, isso significa, principalmente, duas mudanças fundamentais para o mercado financeiro: que passa a haver a inversão do ônus da prova, bem como que o serviço não pode ser ofertado sem prévia solicitação do cliente. O que já tem ocorrido no caso de oferta de cartão de crédito, entre outros.

Para que se compreenda de forma adequada o assunto deve-se tomar como base o uso das Boas Práticas Internacionais, adequadas a realizar a análise e a gestão de risco para essa área de negócios, considerando as obrigações de Responsabilidade Civil e Contratual, Normas do Bacen, Resolução da Anatel sobre SMP, Código de Defesa do Consumidor, ABNT NBR ISO/IEC 27002:2005, ABNT NBR ISO/IEC 27002:2006, ABNT NBR ISO/IEC TR 18044-1:2004, ABNT NBR 15999-1:2007 e ABNT NBR ISO/IEC 20000:2008, Lei de Interceptação n. 9.262/96, Lei de *Software* n. 9.609/98, Basileia II e FINRA Regulatory Notice 10-06 (Social Media Web Sites).

É importante salientar que as medidas de blindagem legal da operação estão diretamente relacionadas ao modelo a ser adotado, uma vez que há uma dependência direta dos parceiros de telecomunicações e telefonia celular¹⁹⁷, tanto da operadora como do próprio fabricante do aparelho.

196. "CÓDIGO DE DEFESA DO CONSUMIDOR. ART. 5º, XXXII, DA CB/88. ART. 170, V, DA CB/88. INSTITUIÇÕES FINANCEIRAS. SUJEIÇÃO DELAS AO CÓDIGO DE DEFESA DO CONSUMIDOR, EXCLUÍDAS DE SUA ABRANGÊNCIA A DEFINIÇÃO DO CUSTO DAS OPERAÇÕES ATIVAS E A REMUNERAÇÃO DAS OPERAÇÕES PASSIVAS PRATICADAS NA EXPLORAÇÃO DA INTERMEDIÇÃO DE DINHEIRO NA ECONOMIA [ART. 3º, § 2º, DO CDC]. MOEDA E TAXA DE JUROS. DEVER-PODER DO BANCO CENTRAL DO BRASIL. SUJEIÇÃO AO CÓDIGO CIVIL" (STF, Tribunal Pleno, ADIn 2.591/DF, rel. Min. Carlos Velloso, j. 7-6-2006, DJ 29-9-2006).

197. ANEXO À RESOLUÇÃO N. 477, DE 7 DE AGOSTO DE 2007

REGULAMENTO DO SERVIÇO MÓVEL PESSOAL — SMP

Art. 6º Respeitadas as disposições constantes deste Regulamento bem como as disposições constantes do Termo de Autorização, os Usuários do SMP têm direito a:

I — liberdade de escolha de sua prestadora;

II — tratamento não discriminatório quanto às condições de acesso e fruição do serviço e das facilidades e comodidades adicionais;

III — informação adequada sobre condições de prestação do serviço, facilidades e comodidades adicionais e seus preços;

IV — inviolabilidade e sigilo de sua comunicação, respeitadas as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;

V — conhecimento prévio de toda e qualquer alteração nas condições de prestação do serviço que lhe atinja;

VI — obter, mediante solicitação, a suspensão do serviço prestado;

VII — não suspensão do serviço sem sua solicitação, ressalvada a hipótese de débito diretamente decorrente de sua utilização ou por descumprimento de condições contratuais ou de deveres constantes do art. 4º da LGT;

VIII — prévio conhecimento das condições de suspensão do serviço;

IX — privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora;

X — resposta eficiente e pronta, pela prestadora, às suas reclamações, solicitações de serviços, pedidos de informação, consultas e correspondências;

XI — encaminhamento de reclamações ou representações contra a prestadora junto à Anatel, outras entidades governamentais ou aos organismos de defesa do consumidor;

XII — reparação pelos danos causados pela violação dos seus direitos;

XIII — obter, gratuitamente, mediante solicitação, a não divulgação ou informação do seu Código de Acesso para a estação de telecomunicações chamada, respeitadas as restrições técnicas;

XIV — não divulgação de seu nome associado a seu Código de Acesso, salvo expressa autorização;

XV — substituição do seu Código de Acesso, desde que haja viabilidade técnica, sendo facultado à prestadora a cobrança pela alteração;

XVI — portabilidade de Código de Acesso, observadas as disposições da regulamentação;

XVII — manutenção, quando de seu interesse, do seu Código de Acesso quando a prestadora promover mudança de padrões de tecnologia ou quando da mudança entre Planos de Serviços de uma mesma prestadora;

XVIII — não ser obrigado a consumir serviços ou a adquirir bens ou equipamentos que não sejam de seu interesse;

XIX — ter restabelecida a integridade dos direitos relativos à prestação dos serviços, a partir da purgação da mora, nos termos previstos no art. 52;

XX — bloqueio da utilização de quaisquer comodidades ou facilidades não previstas no Plano de Serviço ao qual está vinculado, bem como de serviços de valor adicionado, com a correspondente redução no valor devido pelo Usuário, independentemente de prazo de carência ou multa, ressalvados os débitos já constituídos junto à prestadora;

XXI — obter, gratuitamente, em até 24 horas da solicitação, a interceptação pela prestadora das chamadas dirigidas ao antigo Código de Acesso do SMP e a informação de seu novo código do SMP, inclusive quando este for de outra prestadora do SMP, pelo prazo de 60 (sessenta) dias, a contar da data da rescisão do contrato de prestação dos serviços;

XXII — livre escolha e opção do Plano de Serviço ao qual estará vinculado dentre os oferecidos pela prestadora;

XXIII — transferência de titularidade de seu Contrato de Prestação do SMP;

XXIV — não recebimento de mensagem de cunho publicitário da prestadora em sua Estação Móvel, salvo na hipótese de consentimento prévio.

Art. 89. A prestadora é responsável pela inviolabilidade do sigilo das comunicações em toda a sua rede, bem como pela confidencialidade dos dados e informações, empregando meios e tecnologia que assegurem este direito dos Usuários" (www.anatel.gov.br).

A questão da identidade em ambiente de mobilidade é fundamental, e impacta diretamente a necessidade jurídica de prova de autoria, bem como de garantia de Segurança da Informação.

Em síntese, os principais pontos que devem ser considerados em termos de boas práticas legais e gestão de risco para *Mobile Banking* são:

1) Identidade — a questão da senha — evitar que seja a mesma da agência comum e que não fique registrada no aparelho.

2) Modelo de Mobilidade — se GSM (em que a chave criptográfica deve estar no celular) e/ou WAP (se será a versão 2.0 ou outra mais segura), se *offline* e/ou *online*.

3) Tipos de serviços ofertados — Simples (visualização de saldo, extrato), transacional (pagamento de contas, investimentos, recarga de celular, *e-commerce*), Micropagamento por SMS (dinâmicos, estáticos e promocionais).

4) Segurança da Informação — uso de *token* no celular (baixa-se o aplicativo no aparelho para gerar o número), uso de chave criptográfica, *chip* criptografado, aplicações em VPN, HTTPS, SPOP3, RSA, senha WEP e WPA etc.

5) Informação — aspectos de visualização mais condensados, necessidade de ter um Portal de Mobilidade para tirar dúvidas — FAQ.

6) *Disclaimers* — textos jurídicos que exigem ciência pelo aparelho em que fica guardado o *log*.

7) Termo de uso de serviços — documento jurídico próprio para uso do serviço de Banco Móvel. É fundamental ser um termo próprio, independente do de *Internet Banking* (especialmente por questões próprias de custos do serviço, se será cobrado pelo Banco, se tem tarifa da Operadora).

8) Responsabilidade civil de terceiros — responsabilidade da Operadora, inclusive no tocante a disponibilizar as provas eletrônicas geradas. Modelo de garantias e SLA (nível de serviço) sobre entrega de mensagens transacionais (especialmente na questão do micropagamento por SMS).

9) Considerar ainda a aplicação da Constituição Federal de 1988, em especial o art. 5º, IV, V, X, XII, XIV, do Código Civil, em seus arts. 186, 187, 927 e 1.016, e do Código de Processo Civil nos arts. 131, 332, 334.

10) Incidentes e perícia — uso de *mobile forensics*, análise do SIM (*Subscriber Identity Module*).

A mobilidade é um caminho de evolução natural para muitos negócios, especialmente o relacionado a serviços financeiros. O importante é não repetir no *Mobile Banking* os erros cometidos no *Internet Banking*¹⁹⁸, em que não se fez o preparo prévio e preventivo adequadamente, colocando em risco clientes e Bancos, vítimas de ataques de criminosos que exploram vulnerabilidades básicas de segurança da informação.

O *Social Banking* começou a ganhar força em 2010, principalmente no mercado financeiro no exterior. Com a ajuda das redes sociais, os bancos também querem fazer parte da vida de seus clientes, fazendo com que se tenham com eles relações mais “humanas”. Como foi dito no início deste capítulo, as instituições que desejam participar das redes sociais deverão criar canais oficiais e deixar de forma clara o propósito da sua participação nas redes sociais. Pode ser informacional, em que a instituição financeira fará publicações relacionadas a novidades e notícias; ou relacionamento, para interagir com seus clientes; ou atendimento, para auxílio direto aos clientes em substituição ao SAC (Serviço de Atendimento ao Consumidor) por telefone. Isso é uma vantagem tanto para a instituição quanto para o cliente, já que vivemos a transparência digital corporativa.

Com o advento da Internet, além da figura do *Social Banking*, surgiram também outras iniciativas que envolvem dinheiro, como o *crowdfunding*, que nada mais é do que uma forma de se fazer um financiamento de forma colaborativa para viabilizar determinado projeto. Há, também, a figura dos empréstimos *online* entre pessoas físicas sem a participação de instituições financeiras, todavia essa prática é considerada crime de usura (Decreto n. 22.626, de 7 de abril de 1933), além de ser contrária à Lei de Controle do Sistema Financeiro nacional, que impede que pessoas físicas exerçam atividade econômica financeira.

Uma coisa é fundamental para que as instituições gerem oportunidades com o *mobile* e *social banking* sem que isso represente um aumento do seu risco operacional: investir em conscientização de segurança digital do cliente. Principalmente após o advento da Súmula 479¹⁹⁹ do STJ, bem como o recurso que

198. “INSTITUIÇÃO FINANCEIRA — RELAÇÃO DE CONSUMO — DESVIO DE DINHEIRO VIA INTERNET — FRAUDE — FALHA DO SERVIÇO — RISCO PROFISSIONAL — INDENIZAÇÃO DEVIDA. A instituição financeira deve ressarcir o consumidor pelos danos morais e materiais causados pela falha do serviço caracterizada pelo desvio de dinheiro de conta corrente de cliente mediante fraude praticada por terceiro via internet” (TJMG, Ap. 1.0514.06.021309-7, rel. Des. José Flávio de Almeida, j. 14-8-2007).

199. Súmula 479: “As instituições financeiras respondem objetivamente pelos danos ge-

lhe deu origem, a partir da qual passou a ser possível estabelecer um posicionamento acerca da suposta responsabilidade civil objetiva (mesmo sem culpa) das instituições bancárias frente às operações fraudulentas praticadas por terceiros mal intencionados contra seus clientes.

A seguir passamos a analisar os efeitos dessa nova Súmula, conforme estudo feito pela brilhante advogada Dra. Gisele Arantes, em um trabalho que realizamos em conjunto.

Pois bem, conforme denota-se em inúmeros julgados passados sobre o tema, a Superior Corte de Justiça sempre inclinou-se ao raciocínio jurídico de que a instituição bancária teria o dever de indenizar, caso o ato de terceiro pudesse ser evitado, caracterizando o “fortuito interno”, ou seja, dentro do seu processo operacional.

Com base nesse raciocínio, a instituição bancária somente seria responsabilizada de forma objetiva se pudesse ter *evitado* a fraude, caso em que não teria adotado as cautelas necessárias à segura disponibilização dos seus serviços ao mercado (fortuito interno).

A nosso ver, seria aplicável a interpretação de fortuito interno quando o risco está dentro do perímetro físico ou lógico da operação do Banco, de forma direta ou indireta (mediante terceirizados). Um exemplo disso seria a ocorrência da fraude no caixa eletrônico, em que há grande possibilidade de envolvimento de equipe do prestador de serviço.

Por outro lado, fortuito externo seria o que ocorre fora do ambiente do Banco e, portanto, de seu perímetro de responsabilidade. Por exemplo, o uso de um equipamento com vírus (arquivo malicioso) pelo cliente, a resposta de um cliente a um *e-mail* fraudulento com dados de sua conta e senha, o compartilhamento da senha do cliente com terceiro de sua confiança. Situações estas que já são tratadas em campanhas ostensivas de segurança da informação do Banco voltada para os clientes e que podem demonstrar facilmente que houve negligência (falta de cautela e aplicação das recomendações que o Banco fornece para o uso seguro de seus serviços).

Em que pese o risco da atividade exercida, não se pode afastar as hipóteses em que uma fraude é totalmente inevitável, até mesmo porque, hoje em dia, é impossível atuar contra a performance quase perfeita dos *crackers*, dedicados a explorar e forjar vulnerabilidades na grande rede.

rados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias” (STJ, REsp 1.199.182 — PR, rel. Min. Luis Felipe Salomão, j. 24-8-2011).

Dá a importância da análise caso a caso pelo Judiciário, já que há situações em que, mesmo com todos os mecanismos e recursos disponibilizados pelo Banco, com vistas a oferecer mais segurança aos seus clientes e usuários, não seria possível evitar (ou prever) danos ao consumidor.

De outro lado, o “fortuito externo” (ato alheio ao ambiente e perímetro de responsabilidade do Banco) torna-se a única forma de afastar a responsabilidade objetiva das instituições bancárias. Por sua vez, abre margem a uma mudança no comportamento das instituições financeiras, para, talvez, buscar novas formas de documentar as fraudes que, muitas vezes, acabam sendo facilitadas pelo próprio cliente. Além disso, passa a ser fundamental o investimento em campanhas de conscientização de segurança da informação voltadas para o cliente, com informação clara a esse respeito publicado não apenas no Internet Banking, mas também nos perfis oficiais do Banco nas redes sociais. Ter um canal de educação e um canal de denúncia é essencial para demonstrar para o Judiciário até onde vai a “porta” do Banco e onde inicia a responsabilidade do cliente.

Isso sem mencionar, claro, os casos de autofraude (simulada pelo próprio cliente em sua conta/cartão, visando auferir valores indevidos do Banco), não tão raros, o que cabe exclusivamente à instituição provar que foi vítima do seu cliente mal intencionado.

O que não se pode admitir é que a Súmula 479 sirva de estímulo para que os clientes/usuários deixem de se preocupar com a segurança para a realização de suas transações bancárias.

Tal preocupação demanda maior atenção das instituições bancárias quanto aos recursos adotados para a sua proteção, bem como quanto aos recursos disponibilizados para os seus clientes.

O fato é que, em decorrência do risco da atividade exercida, as instituições bancárias deverão adaptar-se às tendências do Judiciário, buscando apoio dos seus próprios clientes para conferir maior eficácia às ferramentas de segurança que oferece, podendo apurar, cada vez com mais eficiência e mais recursos, a fragilidade possibilitada pelo próprio cliente.

Entendemos que a classificação do caso concreto como “fortuito interno” envolve necessariamente os atos de terceiros que de alguma forma estejam envolvidos na operação do Banco (dentro de seu *supply chain* — que vai dos Correios à equipe de manutenção de caixa eletrônico). Mas, quando o ato ou a omissão for do cliente diretamente, entendemos que não está dentro de fortuito interno, mas sim do externo.

Diante da tendência do Judiciário em reconhecer a aplicabilidade da Súmula 479, na grande maioria dos casos envolvendo operações fraudulentas, entendemos que as instituições bancárias devem aumentar o foco na reeducação dos usuários dos seus serviços quanto ao uso seguro dos serviços, além de continuar investindo em mecanismos que minimizem as possibilidades de fraudes e possam gerar maiores registros (*logs*) das transações, o que permitirá maior rastreabilidade da operação e possibilitará a melhor instrução da prova a seu favor em eventual ação judicial.

O que o novo paradigma imposto pelo STJ busca, na verdade, é que as instituições se empenhem para reduzir os fortuitos internos que possam causar danos a terceiros. Com isso, será possível melhor documentar os fortuitos externos, deixando ainda mais claro quais as responsabilidades do cliente também no que tange à segurança da informação, o que excluiria a possibilidade de condenação.

Passa a ser importante também uma atuação junto aos gerentes, para que realizem uma melhor coleta dos fatos, de forma padronizada, bem como para que tentem obter autorização do cliente para eventual verificação do equipamento utilizado para fins de perícia (coleta e espelhamento do artefacto ou trojan). Cabe ao Banco também realizar mais capacitações de seu time para a coleta adequada de provas quando há incidentes. Ainda é comum haver perda ou deterioração de provas essenciais para eximir a responsabilidade do Banco. Deve-se inclusive cogitar a sua centralização para melhor gestão e governança, criando um Banco de Dados de Inteligência que reúna conhecimento e provas dos casos de fraude.

A referida súmula aumenta a necessidade da capacidade de produção de provas por parte do Banco, bem como de resposta rápida aos incidentes, para realizar o “rastros do dinheiro” e buscar ainda mais o flagrante da quadrilha na boca do caixa. Por certo, o investimento em tecnologias que permitam autenticação mais forte do usuário também deverá colaborar para reduzir os riscos.

A tendência internacional tem sido a de reavaliação dos riscos operacionais dos Bancos, em especial com Basileia III, em que o risco humano (comportamental) tem crescido como indicador para perdas. No tocante às decisões do judiciário, em geral, o ônus de provar que a responsabilidade não é da Instituição Financeira é dela, ou seja, tem sido uma tendência primeiramente responsabilizar para somente excluir a responsabilidade do Banco a partir de uma apresentação exaustiva de prova por sua parte.

8.25. Aspectos legais da terceirização em TI (*Outsourcing*)

O *Outsourcing* hoje não é só de tecnologia, e sim a própria forma de pensar e gerir. Tal decisão, entretanto, traz grandes impactos na esfera jurídica, daí decorre a necessidade de criar uma boa estratégia legal para minimizar riscos e aumentar a competitividade por meio da gestão de terceirizados.

No Brasil, a terceirização surgiu na década de 50. As empresas multinacionais, por uma questão de otimização da atividade-fim, deixaram de exercer certas atividades ligadas à parte administrativa do negócio.

Segundo o International Data Corporation (IDC), terceirização é a palavra do momento em tecnologia corporativa. As motivações são redução de custos ou maior *expertise*. Além disso, na era da Internet o espaço físico deixa de ter importância. Exemplo disso é que todos os sistemas administrativos da IBM para as Américas estão em uma só central de dados em Hortolândia. Há quem afirme que a tendência é o TI começar a ser encarado como um insumo básico (como energia, telecom, água) e passar a ser pago conforme o uso.

Outsourcing é a contratação de uma empresa exterior para execução de serviços geralmente não estratégicos, ou seja, não produz valor agregado para os clientes. A concepção teve origem na área de Tecnologia da Informação. “O *Outsourcing de Sistemas de Informação nas organizações consiste na utilização significativa de recursos humanos e/ou físicos externos, para realizar atividades que, tradicionalmente, seriam executadas por colaboradores e por outros ativos da própria. Em sentido mais restrito, o conceito de outsourcing exige também que haja a transferência para o fornecedor externo da responsabilidade de gestão operacional ou diária do serviço em causa*”²⁰⁰.

Os casos mais frequentes de terceirização são: PCs; Assistência Técnica; Impressão; *Hosting* e Servidores; *Software* Corporativo; Redes; e Equipe *Freelancer* Criação, Programação.

Quais são as desvantagens ou risco desse tipo de contratação? Cumpre lembrar que existem duas espécies de *Outsourcing* com implicações jurídicas: a) De pessoa — contratação de um profissional para realização de um trabalho ou vários, visa ou reduzir custos ou serviço mais especializado. Os riscos desse tipo de contratação é menor do que o *Outsourcing* de negócios, pois aqui, além da responsabilidade civil, há também responsabilidade penal. Mas em contra-

200. Fonte: <<http://www.pts.pt/PTSI/TopNavigation/LinksTop/Ajuda/opq/>>.

partida a empresa (contratante) pode vir a ter problemas de ordem trabalhista. b) De negócio — contratação de uma empresa para “cuidar” do negócio almejado pelo contratante. Nesse tipo, mais comum, os riscos são maiores, pois não há falar em responsabilidade penal de pessoa jurídica, exceto dois casos previstos pela nossa Constituição Federal.

Os riscos assumidos ao aquiescer com *Outsourcing* são diversos e variam conforme a espécie de terceirização; entretanto existe *um* risco inerente a ambos: é a má formulação do contrato ou SLAs (acordo de nível de serviços).

É simplesmente vital para a contratante ter extrema cautela quanto ao SLAs. Um instrumento mal redigido, falta de documentação de processos, cláusulas contratuais muito abrangentes etc. aumentam de forma assustadora, ou melhor, astronômica, o risco.

No instrumento contratual podem-se dirimir dúvidas como: todas as vezes em que o fornecedor realiza um novo trabalho, ele cobra novo *fee* (taxa)?; o provedor de serviço pode subcontratar outra empresa para realizar o trabalho?; o produto final do trabalho é do contratante?

E no *Outsourcing* de pessoas é o contrato que vai estabelecer se determinada pessoa é ou não empregado, fato este importante para o Direito do Trabalho.

A terceirização não é apenas gestão de contratos. Segundo o CIO (*Chief Information Officer*) Marcos Hamsi, em entrevista para a revista *Info Corporate* do mês de fevereiro de 2005, a gestão da equipe é primordial para o *outsourcing* dar certo. Ele afirma que “*se os CIOs e a equipe de TI só administram contratos, que vão trabalhar no cartório. Que vão ser advogados. Não dá para abrir mão da gestão profunda da tecnologia. A empresa não pode saber que você é técnico, mas você, necessariamente, precisa ser. Se não, perde o controle do seu departamento*”. Auditar os serviços que estão sendo prestados também é fator relevante para o sucesso, como afirma Adriana Peixoto Ferreira, CIO da Companhia Vale do Rio Doce, na mesma revista.

A responsabilidade solidária é cada vez maior conforme a conectividade das empresas e seu grau de interdependência operacional. Em vez de o CIO liderar um time de funcionários, são administrados contratos e tecnologia. Qual a vantagem disso? Transformar custos fixos em custos variáveis, riscos em oportunidades. Mas cuidado: o que é relevante pode ser terceirizado; já o que é vital ainda é bom deixar “dentro de casa”. Para tanto, seguem algumas recomendações que devem ser observadas, como: não é recomendada a terceirização dos ativos de tecnologia (servidores e demais equipamentos) e sim apenas a gestão deles, pois no caso de uma evolução tecnológica a empresa contratada

pode propor alterações, mas a decisão fica a critério da contratante; fazer auditoria; definir claramente os níveis de serviço SLAs; não contratar por longo prazo; cláusula de arbitragem — evita a morosidade do Judiciário; cláusula de segurança da informação; estabelecer multa quanto ao inadimplemento de qualquer item do contrato; definir as possibilidades de rescisão contratual na forma unilateral caso ocorra descumprimento de uma obrigação crítica; cláusula de seguro, que defina responsabilidade de cada uma das partes, como, por exemplo, determinada situação em que a contratante paga o prêmio.

A grande dúvida não é se a empresa deve ou não fazer terceirização e sim como vai ser administrada, de tal sorte a reduzir os riscos e aumentar o desempenho do negócio. Vale lembrar que se podem terceirizar riscos, mas não responsabilidades.

Há dois tipos de terceirização com implicações legais: a) de pessoas; b) de negócios (inclui processos e tudo o que tenha a ver com o negócio). Em cada uma delas há benefícios e riscos a serem assumidos. É fundamental avaliar as questões relacionadas ao aspecto de direitos autorais, responsabilidade por ato de terceiro, geração de vínculo trabalhista, confidencialidade, sigilo profissional, exclusividade, não concorrência, retenção de conhecimento, entre outros. Devido ao grande grau de interdependência atual, tem-se estudado o que se conhece por *Multisourcing*²⁰¹, para se evitar ficar refém do fornecedor de uma atividade crítica para o negócio.

Independentemente da escolha que a empresa faça, o importante é analisar todos os cenários possíveis para fazer o adequado gerenciamento dos riscos e ter contratos muito bem escritos e documentados.

8.26. Aspectos legais do *cloud computing*

Virtualização total! Não depender mais de um HD específico para acessar seus dados, pois estão em nuvem, a tão falada *cloud computing* permite o desapego completo do “onde” para a oportunidade do “quando”. Ou seja, quando precisar de uma informação, de qualquer lugar do mundo, basta se conectar e ela estará lá disponível. Como todas as demais ferramentas tecnológicas, a computação em nuvem tem seus benefícios e seus riscos, e sua aplicação deve ser analisada no caso a caso.

201. Ver livro *Multisourcing*, de Linda Cohen e Allie Young, Gartner, Inc. Harvard Business School Press.

Víamos o serviço de *cloud computing* como moda, mas em 2011 observou-se que esse serviço ganhou muita força e deixou de ser moda para ser essencial às empresas.

Existem quatro modelos de implantação de *cloud computing*, quais sejam: (i) *nuvem privada* — administrada pela própria empresa ou por terceiros que ajudam na redução de custos, na qual são empregadas as políticas de acesso aos serviços, provando menor risco por ser privada; (ii) *nuvem pública* — é disponibilizada para o público geral ou para grupos de indústrias, podendo ser acessada por qualquer usuário que saiba a sua localização, havendo o compartilhamento de recursos e limites de customização relacionados com Segurança da Informação, SLAs e Políticas de Acesso; (iii) *nuvem comunitária* — possui a característica de ser dividida em várias organizações, em que há o compartilhamento de diversas empresas em uma única nuvem, coordenada por um conselho que compartilha apenas interesses semelhantes, como requisitos de segurança, podendo existir localmente ou de forma remota e ser administrada por uma empresa da comunidade ou por terceiros; (iv) *nuvem híbrida* — este último modelo é caracterizado por envolver dois ou mais modelos para implantação do serviço de nuvem, a privada e a pública; nesse caso, serão entidades únicas, unidas por uma tecnologia padronizada ou proprietária. É possível a portabilidade de dados e aplicações que exigem uma grande classificação e rotulagem dos dados, para garantir que eles serão atribuídos ao tipo correto de nuvem.

Para a prestação do serviço de nuvem existem três modelos: (i) *Software* como Serviço — SaaS (*Software as a Service*) — são oferecidas ao consumidor aplicações que rodam em uma infraestrutura de nuvem do provedor, acessíveis por vários dispositivos, clientes por meio de uma interface leve como um navegador de Internet. O usuário não gerencia a infraestrutura, somente as configurações de usuário da aplicação; (ii) *Plataforma* como Serviço — PaaS (*Platform as a Service*) — são oferecidas para o usuário maneiras de publicar suas aplicações desenvolvidas ou adquiridas. A infraestrutura da nuvem do provedor é criada por meio de linguagens de programação e ferramentas suportadas. O usuário não gerencia a infraestrutura, mas tem controle sobre as aplicações e configurações do ambiente; e (iii) *Infraestrutura* como Serviço — IaaS (*Infrastructure as a Service*) — são oferecidas para o usuário maneiras de provisionar o processamento, o espaço em disco, redes e demais recursos essenciais em que o usuário consegue instalar *softwares*, incluindo sistemas operacionais e aplicações. O usuário não gerencia a infraestrutura de nuvem, mas tem controle dos recursos provisionados, inclusive algumas configurações de componentes de rede (como, por exemplo, *firewalls*).

O que devemos observar para elaborar contratos de *cloud computing*? Por certo deve haver cláusulas específicas de segurança da informação, de autenticação, de recuperação da informação (*backup*), de guarda de provas eletrônicas (exemplo *logs* de acesso, rastreabilidade), bem como um SLA (Acordo de Nível de Serviço) muito bem elaborado.

Há um receio no tocante a se houver um “apagão digital”, como a empresa conseguirá pegar de volta os seus dados, ter acesso a eles, ainda mais se tiverem ido parar na China, por exemplo. O possível risco de alcance das informações em outro ordenamento jurídico pode sim ocorrer em um cenário de uso de *cloud computing*. Por isso, todas essas questões devem estar muito bem previstas e resolvidas no contrato. Essas novas minutas exigem maior atenção à redação técnico-jurídica, sendo aplicado o conceito “bula de remédio”, ou seja, já prever situações de problemas, de eventuais incidentes, e como solucionar ou conduzir cada um (de quem é a responsabilidade, custo, prazo, outros).

Elaboramos uma lista (roteiro) de indicadores mínimos de análise jurídica que devem ser observados na contratação deste tipo de solução e deve ser usada para levantar um autodiagnóstico de necessidade, bem como fazer uma análise de risco deste tipo de contrato:

- Eu preciso ter acesso aos meus dados de qualquer lugar?
- Eu preciso ter acesso a todos os dados ou só a alguns, rotineiramente?
- Só eu preciso ter acesso ou várias pessoas precisam ter acesso?
- Qual o nível de sensibilidade das informações que precisam ser acessadas?
- Qual a possibilidade de publicidade da informação a ser acessada, ela é ostensiva, confidencial ou ultrassecreta?
- Qual a segurança da informação aplicada ao ambiente pelo fornecedor do serviço de computação em nuvem, considerando que não há só uma máquina ou local a proteger e sim múltiplas máquinas e locais a proteger?
- Qual a segurança da informação aplicada para autenticar quem vai ter acesso às informações pela Internet?
- Qual a segurança da informação aplicada aos dados diretamente, que os acompanha onde eles estiverem (ex.: estarão criptografados)?
- Qual a alternativa apresentada pelo fornecedor em um cenário de apagão eletrônico? Como você terá acesso aos seus dados se a Internet sair do ar? Há uma outra forma planejada (plano de contingência, redundância)?
- Qual o impacto se ocorrer um vazamento da informação acessada?

- Qual o impacto se houver indisponibilidade completa de acesso à informação?
- Quanto tempo você pode ficar sem ter acesso à informação, qual o limite (pelo menos 48h é um tempo mínimo esperado para uma recuperação da informação ou do acesso em si, calculado desde o *bug* do milênio)?
- Está prevista uma redundância do fornecedor, se ele ficar indisponível, vier a sofrer um incidente, tiver decretada falência, concordata, deixar de operar, passar por uma fusão e aquisição, o que ocorre com seus dados (quais os procedimentos previstos nestas situações)?
- E se o próximo *bug* do milênio for uma pane geral na Internet, qual seu plano B?
- O que está previsto no contrato para lhe proteger técnica e juridicamente no uso de computação em nuvem?
- Há um SLA para disponibilidade dos dados, recuperação inclusive em situação de caso fortuito e força maior? Qual a responsabilidade das partes específicas de segurança da informação? Qual a penalidade (o valor é proporcional à necessidade de trazer os dados de volta?)

Com base nas respostas às questões formuladas acima é possível criar um plano estratégico para uso da computação em nuvem da melhor forma possível. Dependendo da empresa, será uma alternativa extremamente econômica e viável, por isso, deve-se fazer uma análise de gestão de riscos, considerando o acesso por esta via de informações temporárias de projetos, de agenda de executivos, de ferramentas para edição de conteúdos, mas usando a mesma com cautela quando se tratar de informação confidencial restrita, secreta ou ultrasecreta. Há como usar este novo recurso da melhor forma possível, só tem que estar muito bem prevista a questão técnico-jurídica relacionada à segurança da informação, principalmente disponibilidade, integridade, confidencialidade, autenticidade, não repúdio.

8.27. As novas regulamentações — Sarbanes-Oxley e Basileia II

Sarbanes-Oxley

A Lei Americana Sarbanes-Oxley foi concebida por dois senadores americanos, Michael Oxley e Paul Sarbanes, e foi aprovada em 2002. Desde então,

é mais conhecida como simplesmente SOX, e tem impactado a operação de diversas empresas, que precisam estar em conformidade.

A lei é bastante abrangente e estabelece padrões mais rígidos para Companhias Públicas Americanas e companhias de capital aberto. A SOX contém 11 títulos, ou seções, e foca principalmente a Responsabilidade Penal da Diretoria. As regras serão propostas pela SEC — *Securities and Exchange Commission* (instituição equivalente à Comissão de Valores Mobiliários) para implementar as novas regras e assim estar em consonância com a lei.

O objetivo maior da SOX é restabelecer e aumentar a confiança do investidor e a sustentabilidade nas organizações.

Algumas das exigências são: que as empresas demonstrem boas práticas corporativas; imponham procedimentos efetivos de governança corporativa; penalidades com imposição civil e criminal internacional; ampliação da cultura de ética profissional; declaração de responsabilidade da administração em estabelecer e manter um sistema de controles internos e métricas efetivas para a avaliação da efetividade dos controles, declaração de auditoria independente certificando a avaliação da gerência, declaração identificando a metodologia/*framework* usada para implementar e avaliar os controles internos.

A base para implementação está na área de TI, pois cerca de 90% dos processos de negócios são controlados por TI. Dessa forma, esse departamento não só será responsável pelo controle de acesso, dados e guarda de históricos, como também terá de autenticar cada passo em cada processo.

As seções 302 e 404 são as mais discutidas dentro da referida legislação. A 302 trata sobre a responsabilidade pessoal dos Diretores Executivos e Diretores Financeiros, enquanto a 404 determina a avaliação anual dos controles e procedimentos internos para fins de emissão do relatório financeiro.

A SOX também é conhecida como a Lei da Responsabilidade Fiscal, e segundo a seção 302, em caso de violação, os diretores, auditores e consultores dessas empresas estarão sujeitos à pena dessa lei, 10 a 20 anos de prisão e multa de até US\$ 5 milhões. Já a seção 404 determina, além da avaliação anual, auditoria independente e emissão do mesmo relatório apartado do relatório descrito em linhas pretéritas.

O COSO (*Committee of Sponsoring Organizations of the Tread-way Commission*), uma organização não governamental dedicada a aumentar a qualidade dos relatórios financeiros por meio da ética nos negócios, fornece algumas recomendações para aderência à SOX. A estrutura recomendada pelo COSO é desmembrar os controles internos em cinco componentes inter-relacionados,

quais sejam: ambiente de controle (a base para todos os requisitos dos controles internos inclui valores éticos dos funcionários), avaliação dos riscos (a identificação e a análise de riscos inerentes que possam impedir o alcance dos objetivos do negócio), atividades de controle (tarefas específicas para minimizar cada um dos riscos detectados anteriormente), informação e comunicação (vias de informação que partem da administração para os funcionários e vice-versa) e, por último, monitoramento (a avaliação e apreciação dos controles internos).

Segundo uma pesquisa McKinsey divulgada pela revista *Info Corporate*, 76% dos executivos pagariam mais pelas ações de empresas que adotam práticas de governança. A expectativa de aumento dessas ações segundo a mesma pesquisa é de 24%.

As penalidades²⁰² impostas aos diretores, auditores e consultores, acrescidas da desvalorização das ações das empresas que não cumpriram ou provavelmente não cumprirão as determinações da Sarbanes-Oxley, são motivações mais que suficientes para demonstrar a importância e o impacto de tal regulamentação²⁰³.

Independentemente da SOX, cada vez mais o mercado exige transparência e conformidade legal. Para isso é essencial ter controle e documentar as tomadas de decisão da empresa adequadamente. Não tem como isso ser feito sem uma gestão adequada dos fluxos de informação. Logo, governança em TI alinhado com blindagem jurídica de seus processos é essencial para se atender a SOX. Mas nada disso será eficiente sem conscientização dos gestores, dos altos executivos. É por este motivo, inclusive, que a SOX exige assinatura de um Código de Ética específico.

Basileia I e II

Atualmente os riscos para as instituições financeiras não são apenas os riscos de crédito ou de mercado, mas também os riscos operacionais. O que ocorreu na realidade foi o surgimento de um novo conceito de risco para as instituições financeiras, em razão justamente de uma série de quebras que

202. Para saber se a empresa foi autuada pela SOX basta acessar o site <http://www.sec.gov/> e acessar a área *litigation releases*. Nos Estados Unidos já existem vários casos de punições, pois o prazo para adequação à norma já encerrou. Para os demais países o prazo era até setembro de 2006.

203. Para entender mais sobre a Lei Sarbanes-Oxley, recomendamos a leitura dos livros *Sarbanes-Oxley and the new Internal Auditing Rules*, de Robert R. Moeller, Ed. Wiley, e *The Sarbanes-Oxley Section 404 Implementation Toolkit*, de Michael Ramos, Ed. Wiley.

ocorreram por não terem sido levadas em conta novas variáveis, que estão relacionadas ao dia a dia operacional, a como são feitas as coisas.

Afinal, um vírus que altere dados de uma transação de compra de dólares, ou ouro, ou valor de ações, pode sim levar uma operadora à falência. Não mais apenas quem é o Presidente, se há golpe militar, se há galinha louca, vaca maluca, ou o que mais aparecer por aí. Hoje, as empresas estão capilarizadas em indivíduos, cujas condutas, por mais que pequenas, podem gerar grandes consequências. Sendo assim, é necessário estabelecer novos controles, novos parâmetros de avaliação de risco, e quem não estiver *compliance* paga mais caro por isso. É por essa razão que, quando falamos em Basileia II, não estamos falando apenas para o mercado financeiro, seus resultados serão sentidos até a ponta, até o estabelecimento comercial, até o portador do cartão de crédito.

Para determinar esses controles e parâmetros foi criada a Basileia II, uma deliberação mundial dos bancos sob os cuidados do *Basel Committee on Banking Supervision* (BCBS)²⁰⁴ em Basel, na Suíça. Visa a padronizar a forma como bancos e agências reguladoras dos bancos analisam risco, aplicando-se também a outros tipos de instituição, como as emissoras de cartões, as financeiras, as corretoras. O que se busca é equacionar o gerenciamento de risco para além das fronteiras físicas, ou seja, para dentro das fronteiras informacionais, conectadas, e em tempo real.

A Basileia I, que foi adotada no ano de 1988, atualmente “caiu” em desuso. Isso porque sua eficácia já não reflete a realidade de risco das instituições. As deliberações sobre a sua sucessora, ou melhor, Basileia II, tiveram início em janeiro de 2001, motivadas principalmente no que cinge aos problemas de arbitragem, tendo em vista a divergência entre requerimentos do capital e os cálculos da economia capital.

O Acordo recomenda “três pilares” — análise do risco e controle (determinação dos requisitos mínimos de fundos próprios para a cobertura dos riscos de crédito, de mercado e operacional), supervisão dos recursos (convergência das políticas e práticas de supervisão que podem originar, nomeadamente, a fixação de requisitos mínimos diferenciados, em função dos perfis de risco ou da solidez dos sistemas de gestão e controle interno das instituições) e moni-

204. O Comitê da Basileia sobre a Supervisão Bancária é um comitê de autoridades de Supervisão Bancária que foi criado pelos presidentes dos bancos centrais do Grupo dos Dez em 1975. Consiste em representantes seniores das autoridades de supervisão bancária e dos bancos centrais da Bélgica, Canadá, França, Alemanha, Itália, Japão, Luxemburgo, Holanda, Espanha, Suécia, Suíça, Reino Unido e Estados Unidos.

toramento do mercado financeiro (prestação de informação ao mercado e ao público em geral, de modo a assegurar maior transparência sobre a situação financeira e a solvabilidade das instituições). Dentro deste trinômio, dois são merecedores de maior destaque: a supervisão e a prestação das informações.

Quanto à supervisão, os supervisores devem dispor de meios para coletar, examinar e analisar informações bancárias, em bases individuais e consolidadas. No tocante aos supervisores, ainda, estes devem possuir meios para validar, independentemente das informações com relação à supervisão, seja mediante inspeções diretas, seja pelo uso de auditorias externas.

Já quanto à prestação de informações, as instituições financeiras (principalmente os bancos) devem manter registros adequados e preestabelecidos com as políticas e práticas contábeis consistentes. Tais informações deverão possibilitar uma avaliação precisa da real condição financeira do banco e de sua lucratividade.

Implementar essas “boas práticas” engloba identificar risco do crédito, risco de mercado, risco operacional etc.; a partir daí, alocar o capital, maneira mais apropriada para cobrir as perdas em potencial. Entre os termos técnicos estão inclusos *perda prevista* (*expected loss*), probabilidade do defeito (*probability of default*), defeito dado como perda (*loss given default*), exposição no defeito (*exposure at default*). Os cálculos desses componentes requerem vasta coleta de dados.

A versão final do Acordo foi lançada em junho de 2004 e a implementação tem prazos que vencem em 2006 e outros a serem cumpridos até 2010. Basileia II significa a oportunidade de também pagar mais barato pelo crédito, quanto menor o risco, menores os juros. Ou estar fora do mercado²⁰⁵.

8.28. Tributos

Como tributar a Internet? Será que ela deve ser tributada? O mundo virtual, em princípio, deve ter as mesmas leis que o mundo real? Se a compra de um produto em uma loja física exige o recolhimento de um determinado imposto, em uma loja virtual deve-se aplicar o mesmo? O uso de nota fiscal eletrônica pode ser um caminho? Mas como controlar o pagamento de impostos em *downloads*?

205. Para aprofundar os conhecimentos sobre Basileia II, recomendamos a leitura do livro *Basileia II — Una nueva forma de relación Banca-Empresa*, de Jorge Soley Sans e Ahmand Rahnama, Ed. McGraw-Hill.

A questão dos tributos é uma das mais polêmicas no mundo virtual. Em qualquer lugar do mundo, o Direito Tributário é totalmente codificado²⁰⁶, porque se aplica a uma área pública em que uma das pontas da relação é o Estado. Este último recolhe dos contribuintes porque tem um motivo, uma destinação para esses recursos que deve visar ao bem comum. Se o Direito Tributário não for amplamente codificado, a população tende a ficar à mercê de um Estado que tributaria em causa própria. A própria origem dos Estados modernos foi motivada, entre outras coisas, pela luta contra os abusos tributários de Estados Absolutistas.

A maior discussão sobre tributos na área digital surge por causa da expansão do *e-commerce*, que trouxe a migração de grande volume de negócios para o mundo virtual. É uma distorção considerar que negócios realizados via Internet necessitam de novos tributos²⁰⁷: se o fato gerador permanece o mesmo, os tributos existentes são perfeitamente aplicáveis aqui. Então, o que motiva a discussão? O foco é a competência de tributar e de receber o tributo.

Entendemos que, por respeito ao Princípio Constitucional que incentiva a Iniciativa Privada, para alguns setores da sociedade deveria ser aplicada uma alíquota diferenciada para as transações virtuais. Nesse sentido, até mesmo para estimular o meio de negócios virtuais, seria recomendável que ela fosse inferior à do mundo real. No entanto, há pessoas que defendem uma alíquota superior em razão do maior risco de sonegação e dos menores custos de infraestrutura e pessoal de empresas virtuais. Ora, ambas as motivações dadas são falaciosas, uma vez que sabemos historicamente que maiores tributos nunca solucionaram a questão de sonegação, nem mesmo no mundo real, e as empresas virtuais são as que mais têm contratado mão de obra, assim como têm um custo de tecnologia e logística até maior do que o de empresas do mundo real.

Uma tributação diferenciada com alíquotas reduzidas contribuiria não apenas para o estímulo ao comércio eletrônico, mas também para tornar mais

206. A estrita legalidade é um dos princípios constitucionais que orientam a instituição e cobrança de impostos: de forma genérica, está contida no inciso II do art. 5º da Constituição Federal que diz: “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”. Apesar de ser suficiente para sujeitar a matéria tributária, quis o constituinte reforçar este princípio especificamente para a tributação, e o fez no art. 150, I: “Sem prejuízo de outras garantias asseguradas ao contribuinte, é vedado à União, aos Estados, ao Distrito Federal e aos Municípios: I — exigir ou aumentar tributo sem lei que o estabeleça”.

207. Veja-se, nesse sentido, que a opinião abalizada da doutrina internacional tende à aplicação do sistema tributário vigente às novas condutas. Nesse sentido, concluiu o *Committee on Fiscal Affairs*, da Organização para a Cooperação e Desenvolvimento Econômico — OCDE: “The key conclusion: the taxation principles that guide governments in relation to conventional commerce should also guide them in relation to electronic commerce”.

competitivo nosso mercado dentro de um cenário de economia globalizada, em que os consumidores virtuais têm muitas alternativas e a concorrência não é apenas local, é global.

É de responsabilidade governamental definir uma estratégia de política pública que estimule a iniciativa privada digital²⁰⁸, permitindo a regularização das empresas virtuais e provocando sua expansão, para atrair pequenas e médias empresas que buscam a Internet como meio de baixar seus custos e aumentar suas possibilidades de negócios. Estimular o comércio eletrônico significa incentivar o surgimento de mais empresas virtuais regularizadas, com imposto mais baixo, exigência de produtos mais baratos e de qualidade.

O principal desafio que surge para os tributaristas é a questão da territorialidade, de estabelecer a competência não só para a cobrança, como para o recebimento dos impostos. Um exemplo simples é a venda de carros via Internet, introduzida no Brasil pelas montadoras e que, de certa forma, reduz a participação dos intermediários, no caso as concessionárias, baixando os custos do produto. Uma das soluções apresentadas é o compartilhamento dos tributos: parte do ICMS²⁰⁹ é recolhida pela unidade da federação em que se situa a montadora, e outra parte pela unidade de onde se origina a compra. Dessa forma, os dois Estados continuam a recolher ICMS, como ocorre quando o comprador adquire, na concessionária da esquina, um carro fabricado em outro Estado.

No caso do setor de serviços, a questão é mais complicada. Normalmente, o ISS²¹⁰ é cobrado no local em que o serviço é prestado; quando não se pode

208. Acreditamos que a aplicação de alíquotas diferenciadas e efetivamente menores surtiriam ótimos resultados na economia como um todo, apesar da aparente diminuição na arrecadação. O primeiro efeito seria a diminuição dos custos de um "negócio virtual", a qual poderia tornar os produtos e serviços prestados pela *web* mais competitivos no mercado e promoveria a criação de mais empresas virtuais, além do aumento da participação de empresas tradicionais nas transações eletrônicas. Num segundo momento, teríamos grande fluxo de empresas virtuais se regularizando, pois não é interessante para nenhum comerciante exercer suas atividades à margem da legalidade, pois com a redução da carga de tributos muitos negócios tornam-se viáveis. Os *sites* de vendas quando devidamente registrados transmitem sensação de segurança para o mercado, o que sem dúvida estimula as vendas. Outro efeito benéfico seria que as empresas deixariam de se registrar em locais diferentes daqueles em que de fato atuam, para recolherem menos impostos, como acontece hoje, já que empresas do Município de São Paulo registram suas sedes em cidades como Barueri, por ser menor a alíquota do ISS. Portanto, tratamento tributário diferenciado para as relações comerciais eletrônicas tornaria nossos produtos mais competitivos, promoveria a regularização da maior parte das empresas, trazendo por conseguinte maior proteção e segurança ao consumidor.

209. ICMS — Imposto sobre Circulação de Mercadorias e Serviços.

210. ISS — Imposto Sobre Serviços.

determinar o local da prestação de serviços, o ISS é cobrado no município em que se situa a sede da empresa²¹¹. No caso de empresas totalmente virtuais, como se pode determinar a sede da empresa? A única solução possível é que esta tenha algum registro no mundo real²¹²; no Brasil, a empresa tem de ter CNPJ, mesmo que não tenha uma sede física. Outra regra do mundo real se aplica aqui: se o prestador de serviços é pessoa física, a empresa contratante recolhe o imposto; se é pessoa jurídica, o próprio prestador de serviço o recolhe.

Mas uma das principais questões que geram discussão em matéria contábil e tributária é a de dar ciência da operação. No mundo real, essa ciência é dada por notas fiscais e livros-caixa, ainda, mas com a própria implementação da Nota Fiscal Eletrônica isso já está mudando²¹³. Na Internet, grande parte das transações ocorre sem nota fiscal ou sem outra forma de registro. No entanto, novamente, como estamos falando de uma sociedade digital que tem como principal característica a tecnologia, sabemos que tudo o que ocorre na rede tem como ser identificado e rastreado. Seria, portanto, uma questão de implantação de *software* específico para que os tributos passassem a ser recolhidos automaticamente em operações eletrônicas, com um risco de sonegação muito menor do que o do mundo real.

De qualquer modo, o fator cultural é importante, já que, de certa forma, sempre a maior prova será dada pela consciência do consumidor de exigir nota fiscal das transações realizadas via Internet. Por isso, é fundamental que haja uma mudança de postura não apenas do Fisco como, principalmente, do consumidor. Aliando-se um *software* específico a uma maior consciência de cida-

211. No nosso ordenamento, o problema do local da prestação do serviço é resolvido pelo Decreto-Lei n. 406, de 1968, que possui caráter de lei complementar em matéria tributária, estabelecendo normas gerais de direito financeiro, aplicáveis aos impostos sobre operações relativas à circulação de mercadorias e sobre serviços de qualquer natureza.

212. Quando o titular de um nome de domínio no Brasil é sociedade prestadora de serviços (civil ou comercial), este deve necessariamente estar identificado nos registros mantidos pelo NIC.br através do CNPJ (art. 2º do Anexo I da Resolução n. 002/2005 do Comitê Gestor Internet do Brasil); desta maneira, pode-se vincular um *site* na Internet a um estabelecimento físico localizado em algum município que seria competente para exigir o ISS do titular do domínio, ou seja, a empresa que de fato presta o serviço.

213. Para saber mais sobre a nota fiscal eletrônica veja a legislação Portaria CAT 104/2007 (http://info.fazenda.sp.gov.br/NXT/gateway.dll/legislacao_tributaria/portaria_cat/pcat1042007.htm?f=templates&cfn=default.htm&cvid=sefaz_tributaria:vtribut), Lei n. 14.097/2005 (http://www3.prefeitura.sp.gov.br/cadlem/secretarias/negocios_juridicos/cadlem/integra.asp?alt=09122005L%20140970000). E também os *sites* <<http://www.nfe.fazenda.gov.br/portal/>>, <<http://www.fazenda.sp.gov.br/nfe/>>, <<http://ww2.prefeitura.sp.gov.br/nfe/>>, <http://www.es-critorioonline.com/webnews/noticia.php?id_noticia=7156&c>, <<http://jus2.uol.com.br/doutrina/texto.asp?id=8717>>.

dania e à necessidade de garantir a segurança nas transações virtuais (associada a um seguro), poderemos ter o ambiente virtual como o local mais eficiente para a realização de negócios, podendo-se tornar muito mais eficiente do que no mundo real.

A Internet é um ambiente que estimula as relações em vários níveis, jamais se configurando como um veículo restritivo. Toda a questão das liberdades hoje pode ser lida por um viés tecnológico, em que a Internet assume o papel de um princípio de liberdade puro. Para que isso não signifique anarquia fiscal, é importante que se protejam as partes envolvidas colocando-lhes obrigações, não agindo como uma terceira parte que restrinja a relação.

É importante ressaltar que a sociedade digital se caracteriza por ser uma sociedade de bens de serviço, na qual um livro²¹⁴ que é acessado, assim como uma música e muitos outros produtos, perde sua característica de bem de consumo tangível e passa a ter uma característica de serviço. Sendo assim, podemos avaliar que há no Direito Digital uma mudança quanto aos critérios de distinção entre o que seriam serviços e o que seria a circulação de mercadorias virtuais²¹⁵. Isso tem total impacto na forma como se entende e distingue a incidência do ICMS e ISS.

214. Em relação ao livro eletrônico, surge uma questão de ordem tributária específica. A Constituição Federal, em seu art. 150, VI, *d*, concedeu imunidade tributária aos livros, jornais, periódicos, bem como ao papel destinado à sua impressão, protegidos como instrumentos de transmissão do pensamento, da liberdade de expressão, da informação e disseminação cultural. A questão é: poder-se-ia pensar em imunidade tributária do livro eletrônico? A princípio, como se trata de um bem virtual, imaterial, não poderia ser tratado como mercadoria, termo que pressupõe a materialidade do bem, portanto não se haveria de falar em incidência do ICMS. Porém, a 1ª Turma do Supremo Tribunal Federal, ao julgar o Recurso Extraordinário n. 176.626-3-SP, fixou o entendimento de que o “*software* de prateleira”, na qualidade de cópia ou exemplar dos programas de computador produzidos em série, pode sofrer a incidência do ICMS. Na verdade, o dito imposto não incide sobre o *software* em si (pois que é bem imaterial), mas no seu suporte físico; refazemos, então, a pergunta original: incidiria o ICMS sobre o livro eletrônico quando este se apresentasse sob a forma de “*software* de prateleira”? Acreditamos que, independentemente da forma pela qual se apresenta, o importante será que o conteúdo é de um livro, o instrumento pelo qual se expressa este conteúdo, seja papel, fita magnética ou CD-ROM, está (segundo a melhor interpretação da norma constitucional) isento de impostos, servindo assim às intenções do constituinte, de incentivar a liberdade de expressão e a disseminação cultural.

215. Toda a doutrina é enfática ao dizer que, para fins de tributação, mercadoria é bem corpóreo (constituído por átomos) móvel e destinado ao comércio. Bens imateriais não podem a princípio ser objeto de tributação pelo ICMS (por exemplo, quem compra legalmente um *software*, na verdade não está adquirindo a propriedade deste, mas está recebendo uma licença do autor para usar o programa). Algumas mercadorias virtuais são de fato verdadeiras prestações de serviços, outras constituem-se em direitos como o de autor. Independentemente da classificação, só podem ser tais bens objeto de incidência tributária se o legislador os prever e sobre eles dispuser, visto que até o momento estão imunes à tributação.

Esta questão faz com que existam peculiaridades no tocante ao aspecto tributário digital, já que devem ser definidas as modalidades de obrigações virtuais relacionadas ao fato gerador dos dois impostos. No ISS estamos diante de uma obrigação de prestar um serviço pessoal; já no ICMS, a obrigação é de entregar alguma coisa. Alguns representantes do Fisco confundem essas definições, e ainda confundem os provedores de acesso à Internet com os provedores de informação. Os provedores de acesso permitem que o usuário navegue na rede e, utilizando seus equipamentos, tenha um endereço para recebimento de *e-mails* e arquivos. Já os provedores de informação²¹⁶ desenvolvem e fornecem informações pela rede. Em alguns casos, os dois tipos de provedores podem ser reunidos numa só empresa. Nos dois casos, estão prestando serviços — portanto, deve ser arrecadado o ISS.

Uma possível solução que enxergamos e que tem muito que ver com a tão falada reforma tributária é a aplicação de um Imposto Único para Transação *Online*, quer comércio de bens, quer prestação de serviços, em que seriam consideradas as recomendações já dadas no tocante à competência de cobrar e receber o imposto. Como vimos, há vários conceitos que devemos repensar em função do comércio eletrônico, tais como a determinação do estabelecimento permanente e do estabelecimento principal; os conflitos de jurisdição; o *borderline* entre serviços e produtos; o anonimato dos contribuintes, entre outros. Entendemos que essas adaptações de conceitos às mudanças da sociedade são um princípio do Direito, que é o de ser capaz de se adaptar aos novos casos concretos sob pena de se tornar obsoleto.

Tomemos como exemplo um *site* de vendas *online*. O *site*, por si só, não é nenhuma propriedade tangível, não podendo, portanto, constituir um “local de negócios”. Por outro lado, o servidor por meio do qual o *website* é operado é parte de um equipamento que necessita de um espaço físico e poderia, portanto, constituir um “local de negócios fixo” da empresa que o opera. No entanto, até mesmo isso está em transformação, com o crescimento do uso de hospedagem virtual. Isso tem criado um instituto de empresa totalmente virtual, inclusive sem qualquer equipamento. Surge, então, a questão jurídica: onde está

216. Uma questão que merece atenção é a dos provedores de informação. A Constituição Federal, em seu art. 150, VI, *d*, concede isenção de impostos a livros, jornais, periódicos e papel destinado à sua impressão. Atualmente existem várias edições *online* de periódicos e jornais, bem como há outros provedores veiculando informações as mais diversas, cujos objetivos são os mesmos dos jornais e periódicos impressos em papel. Haveria então de se considerarem imunes de tributação os provedores de conteúdo e os insumos consumidos no processo de produção de suas publicações virtuais, visto que não há motivo para tratamento diferenciado das publicações reais e das feitas por meios virtuais.

situado o estabelecimento principal da empresa²¹⁷? O regulamento do Imposto de Renda, no Brasil, prevê que o domicílio fiscal da empresa é o lugar da situação dos bens ou da ocorrência dos atos ou fatos que deram origem à obrigação tributária. No âmbito digital, devemos adaptar essa regra para que possa atender ao comércio eletrônico, seja via computador, celular ou televisão.

Se a operação é realizada em diferentes territórios, simultaneamente, há uma necessidade de acordos bilaterais internacionais para que se possa aplicar uma legislação mais uniforme e não se prejudique o livre comércio nem se onere demasiadamente o consumidor.

Quanto à aplicação de um imposto sobre o consumo, reunindo tanto o ICMS como o ISS, a questão sobre de quem é a obrigação de tributar e qual o contribuinte também se coloca; para um bem corpóreo, mesmo que transacionado em meio eletrônico, a solução é mais fácil do que para um bem incorpóreo, acessível em ambiente virtual, ou com existência apenas na Internet, como é o caso da aquisição por *download*.

Como estabelecer um mecanismo eficiente de tributação desses “novos bens”²¹⁸ é uma questão que está sendo resolvida no Direito Digital e que necessita da reavaliação dos institutos jurídicos tradicionalmente conhecidos. É claro que podemos aplicar a legislação atual vigente a muitas das transações efetuadas na *Web*, pois, se o consumidor compra um bem físico de uma empresa com domicílio fiscal certo e determinado, não há nenhum problema.

Acreditamos que uma boa alternativa para ter maior controle é na ponta do pagamento. Nessa situação, não importa muito o que está sendo tributado,

217. A Lei Complementar n. 87, de 1996, em seu art. 11, § 3º, considera, para fins de tributação pelo ICMS, estabelecimento como “o local, privado ou público, edificado ou não, próprio ou de terceiro, onde pessoas físicas ou jurídicas exerçam suas atividades em caráter temporário ou permanente, bem como onde se encontrem armazenadas mercadorias”.

218. A *Implementation Option* n. 181 do Relatório de Discussão de Matérias Fiscais sobre Comércio Eletrônico, que norteou a conclusão do Comitê de Assuntos Fiscais da Organização de Cooperação e Desenvolvimento Econômico — OCDE na Conferência Ministerial realizada em outubro de 1998, em Ottawa, para discutir a tributação do *e-commerce*, de que o fornecimento de produtos digitais não deveria ser tratado como fornecimento de mercadorias, recomenda que “autoridades alfandegárias vêm concluindo que para o propósito de tributação sobre o consumo, o fornecimento de produtos digitais não deve ser tratado como um fornecimento de mercadorias, porque: a) serviços e propriedade intangível podem ser recebidos online em forma digitalizada. Eles são recebidos pelos consumidores diretamente do fornecedor. Eles não estão sujeitos a controle alfandegário nem são transportados na aceção tradicional por um intermediário. Eles não são produtos tangíveis quando recebidos inicialmente pelos consumidores. O consumidor pode criar um produto tangível depois, mas isso depende de sua escolha. b) o Comitê de Assuntos Fiscais, dessa forma, concluiu que, no objetivo de dar certeza sobre o tratamento dos produtos digitais enviados online para propósitos tributários, através de fronteiras internacionais, estes produtos não devem ser tratados como mercadorias”.

o que é uma problemática para que não se tribute a renda em vez do consumo, visto que já existe tributo específico para renda; mas essa alternativa pelo menos impede que uma transação de compra de bens intangíveis passe totalmente despercebida.

Já a tributação do comércio eletrônico no aspecto do lucro auferido por determinado estabelecimento permanente de uma empresa deve observar os tratados e acordos de bitributação²¹⁹ entre o país-sede da empresa e o país onde está localizado aquele estabelecimento. Para países importadores de capital e bens e serviços virtuais, como o Brasil, o assunto repercute na competência tributária e na arrecadação. Os acordos tributários consagram o conceito de “estabelecimento permanente” para permitir a identificação da presença de uma empresa de um país no território de outro e, assim, justificar a tributação de seus lucros. O conceito envolve essencialmente a presença física no país pela existência de “um lugar fixo de negócios” por meio do qual a empresa atua. Com isso, alcançou-se razoável equilíbrio entre as competências tributárias do país de residência da empresa (ou seja, do beneficiário final dos rendimentos) e do país fonte dos rendimentos (país no qual atua a empresa por meio do estabelecimento permanente). A Internet coloca em xeque a própria ideia de um lugar fixo de negócios e a necessidade da presença humana direta para o funcionamento de qualquer equipamento, tornando difícil identificar um estabelecimento permanente conforme definido nos acordos tributários internacionais tradicionais.

A OCDE recomenda que o *e-commerce* não seja discriminado relativamente ao comércio tradicional, no sentido de maior oneração. Ou seja, se não houver encargo ou tributo em uma operação física, não deve haver em uma virtual. Assim como não se pode elevar alíquota só por ser na Internet. É lícito supor que deve haver equilíbrio entre os interesses dos Estados de residência e de fonte como acima definidos, quando se acordarem regras tributárias para o comércio eletrônico. Algumas discussões têm enfatizado aspectos particulares, como a caracterização dos provedores e servidores de Internet e *web-sites* como estabelecimentos permanentes, negligenciando um ponto fundamental: a ameaça de que a competência para tributar os lucros do comércio eletrônico venha a se transferir dos países que se tornarão principalmente importadores de bens intangíveis e serviços, que são a maioria e hoje ainda

219. A Convenção Modelo para a Bitributação da Organização para a Cooperação e Desenvolvimento Econômico — OCDE define estabelecimento como “a *fixed place of business through which the business of a enterprise is wholly or partly carried on*”.

abrigam estabelecimentos permanentes, para aqueles poucos países que já sediam as empresas produtoras de tais bens e serviços. Segundo, se, no caso de produtos tangíveis comercializados via Internet, o país que perde o antigo estabelecimento permanente perde também o imposto que teria incidido sobre os lucros daquele estabelecimento, mas ainda arrecada algo na importação. No caso de bens intangíveis e serviços, o país perde receita duplamente, pois não há lucros nem produtos a tributar.

A tributação na fonte pagadora tem sido a regra na legislação brasileira, significando, por exemplo, que a prestação de serviços em geral a um residente no Brasil é alcançada pela tributação, independentemente de onde seja prestada. Nesse contexto, é razoável afirmar que, como regra, a fonte pagadora dos serviços e *royalties* não se deslocaria para um paraíso fiscal, já que isso impediria a dedução dos respectivos custos quando da apuração dos resultados da empresa beneficiária dos serviços.

Um exemplo de caminho de solução tributária que tem sido praticado é o caso da indústria automotiva, que estabeleceu alguns critérios próprios para a cobrança do ICMS no faturamento direto de veículos pela Internet. No caso do faturamento direto, o ICMS é totalmente recolhido no Estado em que o bem é produzido. O que se tem proposto é que o Estado produtor fique com uma parcela e o Estado em que a mercadoria é adquirida, com outra parcela, como acontece no sistema tradicional de venda com a intermediação da concessionária. Nas compras pela Internet, o faturamento será feito diretamente da fábrica para o consumidor, com a eliminação de uma etapa de cobrança do PIS-Cofins, e incide toda vez que uma mercadoria é comercializada. A etapa eliminada é a do varejo.

É importante ressaltar que o aspecto tributário aplicado aos novos serviços e modelos de negócios da era digital precisa ser reavaliado. Isso porque há muitas situações em que, dependendo da forma de execução do uso, ou da materialização do objeto (muitas vezes intangível), enquadra-se como serviço, por exemplo, o *download* de um *software*, enquanto a venda do mesmo *software* em um CD-ROM em uma caixa na prateleira de uma loja já deve recolher o ICMS. Isso sem falar nas discussões sobre tributação de VoIP, que difere do padrão de telefonia, e assim por diante.

No caso específico de *software*, que tem sido objeto de discussão recorrente, devemos observar, em linhas gerais, o seguinte:

Como visto, as conflitantes manifestações jurisprudenciais motivaram a repartição da arrecadação tributária sobre o mesmo fato gerador, além de gerar conflito de competência entre os entes federativos.

De um lado, a distribuição em larga escala do *software* e sua exposição em “prateleiras”, segundo manifestações de nossos tribunais, ensejaria tributação pelo ICMS, por caracterizar operação de compra e venda.

Por outro lado, o desenvolvimento personalizado de *software*, de acordo com as necessidades do contratante, gera a incidência do ISS, arrecadado pelos Municípios e pelo Distrito Federal.

Assim, observando o art. 146, I, da Constituição Federal e para afastar o conflito de competência, o legislador editou a Lei Complementar n. 116/2003²²⁰, que trata do Imposto sobre Serviços de Qualquer Natureza e estabelece o seguinte:

“Art. 1º O Imposto sobre Serviços de Qualquer Natureza, de competência dos Municípios e do Distrito Federal, tem como fato gerador a prestação de serviços constantes da lista anexa (...)

(...)

1 — Serviços de informática e congêneres.

1.01 — Análise e desenvolvimento de sistemas.

1.02 — Programação.

1.03 — Processamento de dados e congêneres.

1.04 — Elaboração de programas de computadores, inclusive de jogos eletrônicos.

1.05 — Licenciamento ou cessão de direito de uso de programas de computação.

(...)”.

No mesmo sentido, a Lei municipal n. 13.701/2003, editada em São Paulo, traz as mesmas disposições do mencionado diploma acima indicado, corroborando a incidência do ISS sobre a operação em análise.

Da legislação aplicável ao tema, outra não poderia ser a solução senão a incidência do Imposto sobre Serviços de Qualquer Natureza, já que, com exceção do direito de uso do *software*, não há transferência de titularidade de direitos, nem sequer o preenchimento dos requisitos da compra e venda.

Considerando a manutenção da titularidade do *software* pelo seu desenvolvedor, não há espaço para a incidência do Imposto sobre Circulação de Mercadorias, por força da combinação da disposição trazida pela Lei Complementar n. 116/2003 com o art. 9º da Lei federal n. 9.609/98²²¹, que determina

220. <https://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp116.htm>.

221. “Art. 9º O uso de programa de computador no País será objeto de contrato de licença.”

a celebração de contrato de licença ou cessão de uso nas relações entre usuário e desenvolvedor.

Outra solução implicaria grave ofensa à ordem tributária nacional, não podendo persistir a validade da jurisprudência que emana do período precedente à edição daquela Lei Complementar, assim como deve ser combatida a atividade fiscal que contrarie tal entendimento.

Dependendo do modelo de contratação, pode ser caso de ISS, de ICMS, ou pode não incidir imposto algum. Por esses motivos acima expostos, é essencial fazer um planejamento fiscal desde o início da operação ou da empresa, para ver qual o modelo mais eficiente e adequado, e assim evitar erros de interpretação que podem aumentar a carga tributária sem necessidade.

Portanto, novamente, não há que falar em lacuna jurídica. O que é preciso, sim, é estabelecer novos padrões e procedimentos de conduta mais adequados à nova realidade da sociedade digital, entre eles pensar em uma tributação diferenciada que estimule os negócios virtuais em vez de onerá-los e terminar por incentivar a sonegação como artifício de sobrevivência e competição num mercado globalizado em que a carga tributária dos outros países é muito menor do que a enfrentada pelos empresários brasileiros.

8.29. Fisco Digital — do SPED à Nota Fiscal Eletrônica

Há alguns anos, a vida dos brasileiros contribuintes de imposto de renda mudou quando a Receita Federal passou a aceitar declaração pela Internet²²².

222. Dicas para fazer a declaração do IR pela Internet:

- fazer uso de computador seguro e conexão segura (é fundamental que tenha antivírus, *firewall* e *patches* de segurança do navegador atualizados);
- evitar fazer a declaração em *cybercafé* ou *lanhouse* (se não houver certeza da segurança do equipamento). Se fizer uso de um computador que seja multiusuário ou coletivo, lembrar de apagar as informações que são geradas pelo *site* da Receita na máquina e de salvar o arquivo digital (comprovante da declaração) em um *pen drive* (para não esquecer no equipamento);
- não deixar para o último dia (pois é comum haver problema de excesso de solicitações ao *site* da Receita e até de indisponibilidade);
- guardar o seu arquivo digital gerado ao final pelo prazo mínimo de 5 anos;
- se possível, fazer uso de um e-CPF (que é uma garantia maior de autoria e identidade e evita alguns riscos na declaração);
- não responder nem clicar em *e-mails* que digam que houve um problema com sua declaração. Em caso de dúvida, entrar em contato direto com a Receita pelo *site* ou pelo

O que isso muda na realidade das empresas com o Judiciário e o Fisco brasileiros mais digitais? O que as empresas devem fazer para atender a esta nova realidade, cada vez mais eletrônica e de menos papel e burocracia? Será que todas as empresas estão preparadas para esta comunicação em tempo real com as autoridades? Será que o apego ao papel é tamanho que nos sentimos inseguros sem ele? Qual o investimento necessário para atender às normas já em vigor que exigem a gestão eletrônica contábil e financeira, bem como do próprio jurídico? Será que pode ser um fator impeditivo para pequenas empresas?

Um dos primeiros requisitos que observamos é a exigência de uso de um certificado digital com base na ICP-Brasil²²³. Que, em princípio, por toda sua característica de aumento de blindagem jurídica, não repúdio, inversão de ônus da prova, já deveria há tempo ter sido adotado maciçamente pelas empresas, o que ainda não ocorreu. Por quê? Talvez por não ser obrigatório para tudo. É uma opção para obter mais informações pelo *site* da Receita Federal, evitando ter de ir presencialmente a uma Secretaria, facilita a retirada de certidões, motivos estes que já provocaram a adesão grande de contadores e financeiros, mas a falta de cultura de uso ainda provoca a sua pouca aceitação em geral.

Imagem então o desafio em se exigir que um pequeno comércio ou varejo tenha um certificado digital? Ou mesmo um correspondente bancário? Quando muito, os bancos conseguem exigir o uso de um *token*. Mas, se se tornar mandatário, por lei, então todos passam a usar. E talvez isso venha a ocorrer nos próximos anos, com toda esta grande virtualização das relações com autoridades, com o e-Gov em geral, que abrange, inclusive, o incentivo ao uso do pregão eletrônico, entre outros.

Uma outra questão relevante em termos de requisitos técnicos para uma empresa operar *online* com as instituições públicas é o uso de um sistema de solução fiscal integrado com um ERP. A exceção de grandes empresas, muitas não possuem este tipo de estrutura ainda bem implementada, o que pode determinar a ocorrência de uma série de incidentes, inclusive de exteriorização de dados equivocados ao Fisco, por conta das exigências do SPED, bem como da nota fiscal eletrônica.

Em 22 de janeiro de 2007 iniciou o Sistema Público de Escrituração Digital (SPED) que foi implementado pelo Programa de Aceleração de Cres-

telefone de atendimento ao público. Acesse o *site* da Receita pois lá há informações sobre os novos golpes, para que você não se torne um laranja digital.

223. A IN 969 da Receita Federal determina que, a partir de 2010, as empresas de lucro presumido devem enviar declarações e demonstrativos com certificado digital.

cimento (PAC 2007-2010) do Governo Federal, como parte das medidas de aperfeiçoamento do sistema tributário e remoção de obstáculos burocráticos ao crescimento econômico (Decreto n. 6.022/2007). O mesmo é constituído de três elementos: Escrituração Contábil Digital (ECD), Escrituração Fiscal Digital (EFD) e Nota Fiscal Eletrônica (NF-e).

A ECD foi instituída pela IN RFB 787/2007 e é o envio de informações contábeis (razão, balancetes diários, balanços, fichas de lançamento e auxiliares e outros) em forma digital, visando à substituição dos livros físicos e sua eventual extinção. Já a EFD é um arquivo digital com informações referentes às operações, prestações de serviços e apuração de impostos do contribuinte. Contém os seguintes Livros Fiscais: Registro de Entradas, Registro de Saídas, Registro de Inventário, Registro de Apuração do IPI, Registro de Apuração do ICMS. E no tocante à NF-e, ela já é uma realidade no Brasil desde o Ajuste SINIEF n. 07/2005. Atualmente é regulada pelo ATO COTEPE n. 14/2007 e o Protocolo ICMS n. 10/2007.

A tendência, por certo, é cada vez mais o Fisco ser digital, mas passamos a enfrentar uma nova questão quando isso começa a acontecer: qual o limite para este poder fiscalizador eletrônico do Fisco que agora está dentro da TI das empresas, com dados sendo exteriorizados em tempo real? Podem haver autuações também simultâneas? Passamos também a alinhar questões de segurança da informação aplicadas a estes ambientes dentro do perímetro da autoridade fiscal e do Poder Público, bem como a questionar os limites de uso e interpretação deles, que não podem ser arbitrários nem tampouco ilimitados.

8.30. *E-Government* e a Administração Pública na Era das Redes Sociais

Não apenas a economia está se tornando cada vez mais digital. Os governos também. No âmbito de Direito Administrativo, os princípios de publicidade dos atos públicos e probidade administrativa fazem com que a Internet seja um meio extremamente adequado para não apenas publicar o que está sendo feito²²⁴, mas também para funcionar como um canal direto de comunicação com cidadãos e contribuintes. Da mesma forma que é aplicado para as operações bancárias o uso de meios eletrônicos reduz muito o custo das tran-

224. O governo brasileiro já tem 100% de suas compras divulgadas na Internet e oferece mais de 800 serviços *online*.

sações, para o governo o meio eletrônico possibilita realizar a um baixo custo os procedimentos licitatórios²²⁵, além de dar maior transparência a eles.

No Brasil a declaração de imposto de renda já é feita em sua quase totalidade pela Internet, assim como a Câmara dos Deputados e a Assembleia Legislativa se tornaram, de certo modo, mais transparentes, com a existência na rede, permitindo o acompanhamento de Projetos de Lei, votações *online* no sistema de “e-Vote”, entre outros.

É inegável que o formato digital promove maior visibilidade, o que possibilita, indiretamente, maior transparência e controle da sociedade sobre aquilo que está sendo feito pelo ente público. No entanto, as mesmas preocupações quanto à segurança e a documentação eletrônica adequada das operações do setor privado devem ser tomadas também pelo setor público.

Na América Latina já existem algumas experiências de *e-Government*, sobretudo no Chile, que criou o portal Trámite Fácil (www.tramitefacil.gov.cl), no qual o cidadão pode obter informações sobre 170 órgãos públicos, e serviços que vão desde a declaração do Imposto de Renda até a emissão de certidão de nascimento. Já nas relações G2B²²⁶, o México foi o pioneiro quando, em 1996, criou o *site* Compranet (www.compranet.gob.mx), no início meramente informativo, mas atualmente já intermediou centenas de licitações. Inspirado na experiência mexicana, o Chile também criou seu portal, o Chile-compra. Ambos os projetos foram selecionados como boas práticas de governo eletrônico pelo programa de cooperação técnica da Organização dos Estados Americanos (OEA).

O setor de compras pela Internet é um dos que mais crescem atualmente, sobretudo por dois motivos: o primeiro é que o processo de compra chega a reduzir em até 95% os custos²²⁷, e o segundo está relacionado com a transparência das licitações. Este é um ponto muito importante quando levamos em conta que os países da América Latina perdem anualmente somas consideráveis com esquemas de corrupção e fraudes nos processos licitatórios.

225. Atualmente as licitações pela Internet são regulamentadas pelo Decreto n. 3.555, de 8 de agosto de 2000, que aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns; e pela Lei n. 10.520, de 17 de julho de 2002, que institui, no âmbito da União, nos termos do art. 37, XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

226. *Government to Business* — Governo e Empresas.

227. Paulo Sérgio Dutra, diretor do setor de *e-government* da consultoria brasileira Stefanini. Publicado na revista *América Economia*, de 16 de agosto de 2001, p. 42.

É, porém, nas relações G2C²²⁸ que os países estão encontrando mais dificuldades. Se por um lado, ao oferecerem uma gama de serviços *online*, os governos fortalecem a democracia, por outro lado esbarram na falta de penetração que a Internet tem nos países da América Latina, em um cenário de “exclusão digital”. Por isso, os projetos de inclusão digital são fundamentais, para evitar que se marginalize o cidadão que não consegue ter acesso aos serviços públicos pela Internet, o que provoca ainda um reflexo mais profundo no tecido social, que é o analfabetismo digital.

O Brasil vem tentando enfrentar essa exclusão digital²²⁹ atuando em duas frentes: uma trabalha a questão da educação; a outra, o acesso às máquinas, por meio da produção de equipamentos a um custo acessível e a instalação de terminais de computadores nas repartições públicas. Um projeto interessante foi posto em prática pela prefeitura de Santo André, no Estado de São Paulo — o Projeto Rede Fácil —, considerado uma das 100 melhores experiências mundiais pelo Habitat, Centro das Nações Unidas para Assentamentos Humanos. Sem custar muito, o projeto oferece 180 diferentes serviços, como solicitação de consertos ou segunda via do IPTU (Imposto Predial Territorial Urbano), tudo sem excluir a parcela da população que não tem acesso à Internet, porque, além do serviço *online*, a prefeitura criou postos de atendimento e disponibilizou o serviço também pelo telefone.

Conforme Florência Ferrer, o Governo Eletrônico pode ser entendido como o conjunto de serviços e o acesso a informações que o Governo oferece aos diferentes atores da sociedade civil por meios eletrônicos. É uma das iniciativas de transformação de uma sociedade industrial em sociedade da informação²³⁰.

Se, para todos os países, o governo eletrônico é uma indiscutível ferramenta de cidadania e de aumento de eficiência da máquina pública, para os países emergentes sua função é ainda mais importante: é uma indiscutível ferramenta de desenvolvimento.

Entrar na economia digital não é uma opção, é uma tarefa indiscutível dos governos. O Brasil é líder dos países emergentes em relação ao tema governo eletrônico e tem um papel orientador para os países da América Latina e para os outros países emergentes.

228. *Government to Citizen* — Governo e Cidadão.

229. Nesse sentido, ver: Marco Maciel, *Avanço Digital e Hiato Social*, que trata do problema da exclusão digital, das formas de combate e da atuação do Governo.

230. *E-Government*, organizadoras Florência Ferrer e Paula Santos, São Paulo: Saraiva, 2004, Introdução, XVII.

Todavia, têm crescido os ataques a *sites* de Governo, principalmente porque os mesmos são extremamente vulneráveis, não foram criados dentro de uma estratégia de plano de contingência e continuidade, visto que no início eram meramente institucionais. Mas evoluíram para se tornar verdadeiros ambientes de governo eletrônico, prestando serviço essencial ao cidadão, e não pode ficar indisponível, não pode sofrer interrupção, muito menos vazamento de dados.

Apesar de estar em vigor o Decreto n. 3.505/2000, uma pesquisa feita pelo Tribunal de Contas da União em 2010 mostrou que a maioria das instituições públicas ainda não possui política de segurança da informação implementada, com campanha de conscientização realizada. Há a nítida impressão de que isso ainda não ocorreu, passados mais de 10 anos, visto que aumentar o nível de monitoramento nos ambientes da administração pública pode vir a revelar condutas indevidas do próprio gestor público, e que ficariam então mais expostas, além da dificuldade de dar continuidade nesse tipo de tema, que exige um trabalho permanente e não se encerra com um mandato.

O Brasil é o único país no mundo que tem votação eletrônica em todo o território nacional. E já se iniciou a discussão para implementação da urna biométrica. Existem cinco níveis de classificação do governo eletrônico, a saber: 1) *institucional*: nesse nível, o Governo deve prover informações ou serviços à comunidade; 2) *transacional*: serviços oferecidos pelo governo que geram uma transação financeira ou um processo transacional, como a declaração do imposto de renda e seu pagamento eletrônico, assim como os pregões eletrônicos, pelos quais o governo faz suas aquisições de materiais e serviços (ex.: *site* ComprasNet e Bolsa Eletrônica do Estado de São Paulo — ressaltamos que em nenhum desses *sites* existe qualquer Política de Privacidade, Segurança da Informação ou Termo de Uso de Serviços, que são documentos legais essenciais para a gestão do risco digital); 3) *colaborativo*: em um portal do Governo, podem ser fornecidos quase todos os serviços por ele prestados; 4) *integração entre todos os níveis*: permite que os dados necessários para uma transação ou o andamento de um processo administrativo sejam provenientes de todas as bases de dados do governo e sistemas estruturados sejam compartilhados; e 5) *personalização total*: o cidadão interage com o Governo de forma customizada e personalizada.

A tecnologia da informação é uma importante aliada dos governos na luta por uma sociedade mais justa em direitos e oportunidades. E o Brasil é rico em exemplos de como melhorar a qualidade de vida dos cidadãos e tornar o Estado mais eficiente com a ajuda dos avanços da computação e da Internet.

Mas a tecnologia não é neutra: altera e muda a forma dos processos que a recebem, torna-se um paradigma organizacional que cada organização deve conjugar em seu contexto peculiar.

Sobre as necessidades de inovações e do uso correto de ferramentas na gestão de negócios no setor público, diz David Osborne, teórico em gestão pública: *“O desperdício no Governo é extraordinário, mas não podemos evitá-lo examinando orçamentos e eliminando alguns de seus itens. Como notou um observador, nossos governos são pessoas obesas que precisam perder peso: elas devem comer menos e fazer mais exercício. Mas quando falta dinheiro, o que se faz é cortar alguns de seus dedos. Para derreter a gordura, precisamos mudar os incentivos básicos que orientam nossos governos. Precisamos transformar instituições burocráticas em instituições inovadoras, dispostas a eliminar iniciativas obsoletas, prontas a fazer mais com menos recursos, interessadas em absorver novas ideias”*.

O maior desafio do governo brasileiro é assegurar a atualização tecnológica da própria Administração Pública, num contexto de mudança e inovação aceleradas, sobretudo por meio da identificação e da gestão das competências essenciais ao governo eletrônico²³¹.

O que pode ser feito, em caráter emergencial, para melhorar o nível de proteção do ente público e também dos dados dos cidadãos brasileiros, que devem ser cuidados por essa instituição, são: a) revisar nível de segurança da informação dos *sites* de governo, melhorando programação dos códigos-fonte e criptografando bases de dados; b) implementar plano de contingência e continuidade e demais medidas para evitar interrupção; c) realizar monitoramento permanente do ambiente, podendo usar estratégia *honey pot* para pegar um ataque logo no início e identificar seu autor; criar policiamento *online* (não apenas a delegacia de crimes eletrônicos); d) aprovar leis que melhorem tipificação e guarda de provas, devendo trazer os novos tipos de crime eletrônico, cyberterrorismo e guerra cibernética; e) definir modelo de identidade digital obrigatório e prazo mínimo de guarda de dados de conexão e tráfego por provedores de internet, *e-mail*, páginas de conteúdo, redes sociais; f) implementar campanha de conscientização de segurança da informação pública, voltada aos servidores e ao cidadão, orientando sobre proteção de senha, bloqueio de estação de trabalho, necessidade de desligar o equipamento quando não estiver sendo usado e de manter atualizados os *softwares* de antivírus.

Com isso, as principais diretrizes do Governo Eletrônico Brasileiro, conforme relatório consolidado de maio de 2004, do CEGE — Comitê Executivo do Governo Eletrônico — presidido pelo Chefe da Casa Civil da Presidência da República, são: a) promover a cidadania e o desenvolvimento; b) funcionar como instrumento de melhoria de atendimento ao cidadão; c) promover a

disseminação da tecnologia da informação como uma forma de apoiar o próprio desenvolvimento do País; d) promover o uso e disseminação de práticas de Gestão do Conhecimento na Administração Pública.

Essa inovadora visão de trabalho no setor público, no âmbito do governo eletrônico, constitui nova capacidade de articulação do processo decisório, de gestão das suas políticas estratégicas e de inclusão de um novo produtor de conhecimento geralmente esquecido: a sociedade e suas organizações. Além disso, os modelos e práticas da gestão do conhecimento são iniciativas essenciais para integração das três esferas de governo.

São, portanto, fatores críticos de sucesso para o governo eletrônico segundo a Unidade de Missão Inovação e Conhecimento — UMIC (www.unic.gov.pt): a) definir uma estratégia focalizada no cidadão; atuar no ponto de atendimento (*front Office*) e nos processos de retaguarda (*back Office*); b) obter forte apoio político e organizacional; efetuar investimentos estratégicos; c) adotar uma postura colaborativa; d) garantir o envolvimento da sociedade civil e o desenvolvimento da democracia eletrônica; e) definir objetivos claros a sua implementação; f) definir padrões técnicos comuns de interoperacionalidade; g) celebrar parcerias com o setor privado; h) implementar técnicas de CRM nos portais de administração pública; i) garantir a proteção da informação — sigilo, segurança e privacidade.

A legislação brasileira inovou recentemente com a Lei de Acesso à Informação (Lei n. 12.527, de 18 de novembro de 2011), que entrou em vigor em maio de 2012. Marco muito importante para a Administração Pública brasileira, essa lei regulamentou as informações que são manuseadas pelo poder público. Vale lembrar que o acesso às informações públicas é uma garantia constitucional à coletividade (prevista no art. 5º, XXXIII, no art. 37, § 3º, II, e no art. 216, § 2º, todos da Constituição Federal). Ainda é importante lembrar que, para que haja o acesso a tais informações, é preciso que exista uma lei específica que regule essa garantia.

As instituições públicas que devem cumprir norma vão desde os órgãos e entidades do poder executivo, poder legislativo, judiciário, até os Tribunais de Contas e o Ministério Público, entre outras entidades, como autarquias, fundações públicas, empresas públicas, sociedades de economia mista e outras controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. Não só entidades públicas que estão sujeitas à norma, mas também as entidades privadas sem fins lucrativos que recebam recursos públicos para a realização de ações de interesse público diretamente no orçamento ou por meio de subvenções sociais, termo de parceria, convênios, contrato de gestão, acordo, ajustes etc.

231. Ver relatório do Governo brasileiro em <www.governoeletronico.gov.br/anexos/E15_90balanco_2anos_egov.pdf>.

Esta lei deseja mostrar transparência do governo quanto ao manuseio de informações pelo governo, também para combater a corrupção, mostrar o funcionamento e demais atos que são omissos por diversos órgãos do governo, além de disponibilizar dados pessoais de quem os solicitar.

Como regra geral, a maioria dos dados e informações é pública. Podemos observar, portanto, que há exceções à norma, verificando-se que haverá casos em que informações terão caráter sigiloso, que possam pôr em risco a segurança pública, como, por exemplo, pesquisas que tenham relevância à saúde pública, mas, ainda em estudo, não podem ser publicadas por estar em fase experimental.

Para ter acesso a tais informações, qualquer pessoa poderá requerer ao órgão que tem interesse. A própria Lei n. 12.527/2011 traz o procedimento administrativo que os órgãos terão de adotar, como criar um canal em que seja possível realizar consultas, devendo estar em um local de fácil localização no *site*, bem como criar uma seção perguntas mais frequentes com respostas sobre o órgão. As solicitações devem estar prontas de imediato, caso contrário, o órgão deverá cumprir no prazo de 20 dias as solicitações feitas, sob pena de levar alguma sanção administrativa.

A lei traz o prazo de segredo de informações, nomeando-as como ultrassecretas, secretas e reservadas, pelos prazos de 25, 15 e 5 anos, respectivamente. Importante ressaltar que as informações ultrassecretas geralmente tratarão de assuntos estratégicos do Governo que são atinentes à presidência da república e aos militares, não sendo possível a sua solicitação por serem informações sensíveis.

A lei também trata da responsabilidade dos servidores que não fornecerem as informações nos casos: (a) de recusar-se a fornecer informação requerida de acordo com a Lei de Acesso a Informações, demorar por vontade própria o fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa; (b) utilizar as informações de forma indevida, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública; (c) agir com dolo ou má-fé na análise das solicitações de acesso à informação; (d) divulgar ou permitir a divulgação de informações ou acessar ou permitir acesso indevido as informações que forem sigilosas ou pessoais, tendo em vista que é um dever do servidor mantê-la em sigilo; (e) impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem; (f) ocultar alguma informação quando houver

a revisão de autoridade superior competente informação que seja sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros; e (g) destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.

No entanto, a nova lei estabelece uma exceção às penalidades previstas na Lei n. 12.527/2011: os servidores não poderão ser responsabilizados civil, penal ou administrativamente por dar ciência, a quem de direito, de informação concernente à prática de crimes ou improbidade. Isso quer dizer que, embora o servidor cometa algum dos ilícitos listados acima, poderá fornecer informações para quem solicitar por ser alguma pessoa autorizada, como um juiz, para solucionar um caso de improbidade administrativa, o servidor não será responsabilizado.

A Administração Pública não quis ficar de fora das redes sociais. Viu-se que nos últimos dois anos esse assunto passou a ser item prioritário na pauta do planejamento estratégico das instituições da Administração Pública. O tratamento desse tema exige cada vez mais equipes treinadas e uso de ferramentas especializadas. Afinal, quando se trata de proteção de marca e reputação, não dá para se ter um “puxadinho digital”.

Logo, estar ou não nas redes sociais deixou de ser uma escolha, marcar presença passou a ser essencial, até para evitar a existência de perfis falsos que pudessem confundir o cidadão e gerar até fraudes. O trabalho de blindagem técnica e legal da marca nesse novo ambiente é importantíssimo. Motivo este que virou tema da recente Portaria n. 38 do Conselho de Defesa Nacional, de 11 de junho de 2012, que passou a exigir um acompanhamento técnico-profissional e próximo do próprio gestor público.

Nessa portaria passou-se a elencar justamente a necessidade de se assumir as redes sociais como novo meio de comunicação entre os cidadãos, mas também a dar o devido tratamento jurídico e de segurança nesses ambientes para as Instituições Públicas da esfera federal. Isso significa ter que atualizar a Política de Segurança da Informação e Comunicações de cada órgão federal e entidades para ter um capítulo específico sobre o comportamento dos servidores e empregados públicos nas redes sociais.

Além disso, passou a ser obrigatória a criação de duas funções específicas: a de “administrador de perfil institucional” e a de “agente responsável”, que têm como responsabilidade administrar os perfis institucionais do órgão ou entidade nas redes sociais e realizar a gestão desses perfis de forma ética e segura. Proibiu, além disso, a terceirização completa da administração desses perfis, dessa forma, estabelece que os canais fiquem sob os cuidados

de pessoas da administração pública federal. Contudo, permitiu a formação de equipes mistas, até pela necessidade de criação de conhecimento, no entanto, sempre com a presença de servidores ou empregados públicos federais ocupantes de cargo efetivo ou militar de carreira do respectivo órgão ou entidade.

Ainda conforme a Portaria, todos os usuários passam a ter que assinar um termo de responsabilidade concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que acessar, bem como assumir as responsabilidades decorrentes de tal acesso.

Como a experiência na esfera privada nos mostra, a questão das redes sociais é extremamente importante e a segurança se passa por educação. Ou seja, há necessidade de investir-se maciçamente na capacitação do Administrador de Perfil e do Agente Responsável, mas também em campanhas de conscientização dos servidores em geral, e em ferramentas que permitam o monitoramento das condutas para uma ação rápida de resposta a incidentes. De nada adianta ter alguém que publique informações nos perfis oficiais e não ter um responsável que monitore o conteúdo publicado, tanto no perfil oficial quanto para as interações com outros perfis.

Por isso o termo de responsabilidade deve tratar desse cenário mais híbrido, de postura ética não apenas no acesso corporativo e no perfil oficial, mas também no acesso particular e nos perfis pessoais, quando envolver assunto da Instituição, reforçando o dever de sigilo profissional, bem como todos os preceitos do código de conduta do servidor público.

Considerando a entrada em vigor recente da Lei n. 12.527/2011, já mencionada, e a Portaria n. 25, de 15 de maio de 2012, que trata dos documentos que devem ser mantidos sob sigilo da Casa Civil, devido ao cumprimento do princípio da publicidade e transparência da Administração Pública, pode haver confusão junto aos servidores públicos do que pode ser publicado ou não nas redes sociais, por isso é fundamental criar um guia a fim de orientar os usuários com exemplos para melhor conscientização das equipes.

Ademais, é fundamental esclarecer qual é o canal de resposta oficial, para reportar os incidentes à área responsável por estes canais de comunicação.

Assim como a iniciativa privada, o Governo só tem como evoluir junto com a própria sociedade digital, por meio da virtualização de seus serviços, permitindo mais acesso e mais transparência.

Como o cidadão brasileiro está cada vez mais nas redes sociais, nos últimos

dois anos esse assunto passou a ser item prioritário na pauta do planejamento estratégico das instituições da Administração Pública.

Com o fenômeno da consumerização e da mobilidade, a segurança da informação precisa evoluir para ser uma segurança mais holística, mais integrada, em nível de perímetro físico, lógico e social. Isso significa que não importa mais quem fornece o recurso, mas sim de quem é a informação e, acima de tudo, a reputação (marca) envolvida. Independentemente de se ter agora uma previsão formal para a gestão oficial dos perfis públicos, é sabido que todos os servidores podem estar publicando informações durante o expediente, pelos seus celulares e *tablets* pessoais, sem importar a rede ou a conexão de *web* da repartição.

Por isso o termo de responsabilidade deve tratar deste cenário mais híbrido, de postura ética não apenas no acesso corporativo e no perfil oficial, mas também no acesso particular e nos perfis pessoais, quando envolver assunto da Instituição, reforçando o dever de sigilo profissional bem como todos os preceitos do código de conduta do servidor público²³².

232. Legislação Aplicável — Aspectos de Responsabilidade:

Art. 37, § 6º da CF:

“As pessoas jurídicas de direito público e as de direito privado, prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.”

Lei n. 8.112/90:

Art. 116. São deveres do servidor:

I — exercer com zelo e dedicação as atribuições do cargo;

II — ser leal às instituições a que servir;

III — observar as normas legais e regulamentares;

IV — cumprir as ordens superiores, exceto quando manifestamente ilegais;

V — atender com presteza:

a) ao público em geral, prestando as informações requeridas, ressalvadas as protegidas por sigilo;

b) à expedição de certidões requeridas para defesa de direito ou esclarecimento de situações de interesse pessoal;

c) às requisições para a defesa da Fazenda Pública.

VI — levar ao conhecimento da autoridade superior as irregularidades de que tiver ciência em razão do cargo;

VII — zelar pela economia do material e a conservação do patrimônio público;

Capítulo IV — Das Responsabilidades

Art. 121. O servidor responde civil, penal e administrativamente pelo exercício irregular de suas atribuições.

O maior desafio é cultural! Vivemos em um país de povo mais comunicativo e com espírito mais jocoso, onde é comum comentar-se rotinas de trabalho, seja no elevador, na mesa de bar ou no *Facebook*. Mas a Sociedade Digital trouxe um agravante para este tipo de atitude: ela documenta muito mais e se perpetua com alcance global e em tempo real. Além disso, devido à maior capacidade de prova, aumenta a responsabilidade do gestor por negligência ou conivência, pois, ocorrido o fato, não fazer nada gera comprovação de omissão intencional.

Art. 122. A responsabilidade civil decorre de ato omissivo ou comissivo, doloso ou culposo, que resulte em prejuízo ao erário ou a terceiros.

§ 1º A indenização de prejuízo dolosamente causado ao erário somente será liquidada na forma prevista no art. 46, na falta de outros bens que assegurem a execução do débito pela via judicial.

§ 2º Tratando-se de dano causado a terceiros, responderá o servidor perante a Fazenda Pública, em ação regressiva.

§ 3º A obrigação de reparar o dano estende-se aos sucessores e contra eles será executada, até o limite do valor da herança recebida.

Art. 123. A responsabilidade penal abrange os crimes e contravenções imputadas ao servidor, nessa qualidade.

Art. 124. A responsabilidade civil-administrativa resulta de ato omissivo ou comissivo praticado no desempenho do cargo ou função.

Art. 125. As sanções civis, penais e administrativas poderão cumular-se, sendo independentes entre si.

Art. 126. A responsabilidade administrativa do servidor será afastada no caso de absolvição criminal que negue a existência do fato ou sua autoria.

Decreto n. 1.171/94

XIV — São deveres fundamentais do servidor público:

q) manter-se atualizado com as instruções, as normas de serviço e a legislação pertinentes ao órgão onde exerce suas funções;

r) cumprir, de acordo com as normas do serviço e as instruções superiores, as tarefas de seu cargo ou função, tanto quanto possível, com critério, segurança e rapidez, mantendo tudo sempre em boa ordem.

Lei n. 8.027/90

Dispõe sobre normas e condutas dos servidores públicos civis da União, Autarquias e das Fundações Públicas e dá outras providências:

Art. 2º São deveres dos servidores públicos civis:

III — observar as normas legais e regulamentares;

VII — guardar sigilo sobre assuntos da repartição, desde que envolvam questões relativas à segurança pública e da sociedade;

VIII — manter conduta compatível com a moralidade pública;

Vivemos a era da transparência corporativa, profissional e pessoal, bem como um excesso de exposição de vida íntima! As redes sociais são mais que um canal de comunicação, como já foi dito, são um canal de documentação, em que o conteúdo pode, sim, gerar responsabilidades para as partes envolvidas. Não há como ficar isento das opiniões que publicamos atualmente. Logo, é importante tomar alguns cuidados para mitigar eventuais riscos.

Deste modo, resumimos o que deve ser endereçado pelos Órgãos e Entidades da Administração Pública Federal, direta e indireta, para atender ao disposto na Portaria e também a um cenário e e-cidadão versão 3.0 que está em mobilidade e nas redes sociais:

PLANO DE AÇÃO — PORTARIA N. 38 — SEGURANÇA NAS REDES SOCIAIS

1. Definir quem será o Administrador de Perfil e o Agente Responsável;
2. Fazer o registro dos perfis oficiais nas Redes Sociais (em especial no *Facebook*, no *Twitter* e no *LinkedIn*);
3. Implementar ferramenta de Monitoramento específico das Redes Sociais (que possa identificar as interações dos perfis oficiais e também o que ocorre fora deles);
4. Elaborar o plano de resposta a incidentes e à crise de imagem digital (já prevendo ações, SLAs, registro e coleta de provas legais, modelo de instauração de processo administrativo ou judicial se necessário, respostas rápidas);
5. Capacitar a equipe interna ou a equipe mista que fará a gestão dos perfis oficiais e a análise dos relatórios de monitoramento;
6. Elaborar e implementar o Termo de Responsabilidade para assinatura dos usuários;
7. Elaborar o Manual de Postura Ética e Segura do Servidor na Rede Social;
8. Realizar a Campanha de Conscientização para os usuários específica sobre o tema das Redes Sociais;
9. Realizar reunião periódica do Comitê de Segurança da Informação e Comunicações para análise de riscos em Redes Sociais, planejamento de ações e implementação de medidas (é recomendável que se reúna no máximo em intervalos de até três meses);

10. Fazer uso de empresas e consultores especialistas em Redes Sociais, Direito Digital, Segurança da Informação para gerar conhecimento e treinar os times internos, bem como apoiar na geração e revisão de toda a documentação.

DICAS PARA AS INSTITUIÇÕES NAS REDES SOCIAIS

- Realizar um planejamento estratégico para fazer o registro e gestão de perfis oficiais da Instituição;
- Defina claramente o propósito: se será meramente institucional, para gerar relacionamento com o cidadão ou realizar atendimento (resposta a dúvidas e recebimento de sugestões e reclamações), pois, no último caso, precisa ficar claramente definido o horário do expediente;
- Elabore um Manual de Postura Ética e Segura nas Redes Sociais e implemente uma campanha de conscientização com foco específico nesse tema;
- Tenha um plano de resposta a incidentes definido. Você deve estar preparado para resposta a uma crise de imagem digital, e tem que ser imediato;
- Transparência. Sempre apresente as informações da maneira mais clara possível e em atendimento à Lei de Acesso à Informação (LAI);
- Cuidado com a publicação de informações confidenciais que possam representar risco à segurança nacional, bem como à soberania, além do que for considerado segredo industrial e segredo de justiça;
- Realizar treinamentos de capacitação com a equipe responsável pela administração dos perfis institucionais;
- Não deixe de responder às mensagens enviadas para o perfil oficial;
- Monitoramento. Ter ferramenta e gerar relatórios de monitoramento das redes sociais;
- Utilizar as redes sociais de acordo os Termos da Portaria n. 38.

DICAS PARA OS SERVIDORES (USUÁRIOS) NAS REDES SOCIAIS:

1. Crie seu perfil para proteger sua identidade digital nesse ambiente e não compartilhe sua senha com outras pessoas;
2. Deixe claro no seu perfil que o propósito é pessoal (particular), para evitar que se confunda uma opinião postada no mesmo com uma opinião da instituição na qual trabalha;

3. Evite associar conteúdo pessoal com o nome ou marca da instituição em que trabalha (ex.: sou fulano de tal da instituição tal e acho isso);
4. Não divulgue informações da sua rotina de trabalho em hipótese alguma (isso abrange atividades, horários, trajetos, nomes de pessoas e nomes de projetos);
5. Não publique informações classificadas como internas ou confidenciais;
6. Não ofenda outros servidores, cidadãos ou fornecedores;
7. Não chame colegas por apelido, pratique uma comunicação mais objetiva e direta;
8. Tenha uma postura ética, segura e dentro das leis nas redes sociais. Dependendo do cargo que ocupar, qualquer manifestação, mesmo que pessoal, pode gerar impacto na sua instituição;
9. Evite o excesso de exposição de vida íntima, em especial fotos;
10. Em hipótese alguma, gere contato ou publique informações que possam configurar manifestação política, campanha de candidato;
11. Respeite os direitos autorais. Sempre cite a fonte ou a referência do conteúdo publicado;
12. Utilize apenas fotos ou imagens previamente autorizadas pelas pessoas nelas retratadas;
13. Na dúvida sobre o que pode ser publicado em rede social, peça autorização antes.

8.31. Justiça Digital — Processo Eletrônico

Nos últimos anos, as decisões judiciais foram aprimorando-se no tocante aos temas de direito digital, especialmente no uso de provas eletrônicas na Justiça. A tal ponto que estamos vivendo um marco histórico que é a migração para o processo eletrônico, ou seja, o juiz ficou digital também!

Não há como se obter uma decisão favorável do Judiciário sem que haja o devido preparo por parte da empresa, unindo medidas jurídicas, técnicas e de recursos humanos, visto que o uso de *e-mail* corporativo, rede, Internet, *smartphone*, *notebook* exige a criação de uma cultura interna nova e um bom senso geral que ainda está sendo estabelecido no dia a dia. E tudo

deve ser documentado. A guarda das provas eletrônicas²³³ com a devida cadeia de custódia é essencial. Porque, em geral, se houver demissão, há

233.

EVOLUÇÃO DO JUDICIÁRIO BRASILEIRO E DA SOCIEDADE EM RELAÇÃO ÀS PRINCIPAIS QUESTÕES DO DIREITO DIGITAL		
ANO	PODER JUDICIÁRIO	SOCIEDADE CIVIL
2000 a 2003	Monitoramento de e-mail: O monitoramento de e-mail é invasão de privacidade.	Monitoramento de e-mail: O monitoramento não era feito ou era feito de forma manual e esporádica, o empregador se responsabilizava pelos atos do empregado e pelo mau uso da informação, não podendo exercer a vigilância por causa das questões de definição dos limites de intimidade.
	E-mail como prova: A utilização do e-mail como prova era restrita. Não serve como prova única, mas pode servir para ajudar as demais provas.	E-mail como prova: Empresa e colaborador possuem dúvidas quanto à admissibilidade do e-mail como prova, e não as utilizam com frequência.
2004 a 2006	Monitoramento de e-mail: O monitoramento de e-mail passa a ser admitido, nos casos em que a empresa comprova que havia ciência prévia do empregado.	Monitoramento de e-mail: As empresas passam a adotar procedimentos mais rígidos para proteção de seus ativos, realizando o monitoramento e adquirindo ferramentas para tal, mesmo que sem a ciência prévia do empregado, ainda sem a existência de política de segurança da informação, ou a previsão tímida em normas esparsas de e-mail e Internet (que não deixavam claro se podia usar para fim pessoal a ferramenta de trabalho).
	E-mail como prova: Passou-se a admitir o e-mail como prova única.	E-mail como prova: Os colaboradores questionam a privacidade no uso, pela empresa, dos e-mails para prova de demissão por justa causa.
2007 a 2009	Monitoramento de e-mail: O monitoramento de e-mail é aceito, já que a ferramenta de trabalho é do empregador e o mesmo é responsável por seu uso indevido por parte de seus empregados.	Monitoramento de e-mail: A empresa possui política de uso dos recursos e política de segurança da informação, aplicando a seus funcionários sempre que necessário. No entanto, ainda há uma zona cinzenta em ambientes de mobilidade, home office e terceirizados, que também precisa estar previsto em normas, códigos de conduta e contratos.
	E-mail como prova: Admissão de novas tecnologias (e-mail, Orkut, Youtube, fotografia digital, mensagens sms etc.) como prova, desde que não haja comprovação de alteração dos dados do e-mail. Ou seja, deve ser preservado de forma íntegra e pode haver perícia no original eletrônico.	E-mail como prova: Tanto as empresas como os colaboradores se valem de provas eletrônicas para fundamentar suas alegações. Não apenas o e-mail, mas também outras evidências eletrônicas.
OUTRAS QUESTÕES ATUAIS EM FRANCO DESENVOLVIMENTO DO DIREITO DIGITAL		
	PODER JUDICIÁRIO	SOCIEDADE CIVIL
Criação de comunidades para falar mal da empresa pelo colaborador.	Os tribunais ainda se furtam a admitir a demissão por justa causa do colaborador quando da criação de comunidades/blogs etc. para falar mal da empresa, fundados na liberdade de expressão e na conduta fora do local de trabalho.	São inúmeras as comunidades/blogs etc. criados por colaboradores para falar mal da empresa. Por isso a necessidade de manter-se políticas rígidas e o monitoramento constante do nome/marca da empresa na Internet.
Ponto eletrônico.	O ponto eletrônico é em regra admitido, mas desconsiderado facilmente ante a presença de prova que o contradiga (inclusive testemunhal).	As sociedades utilizam largamente o ponto eletrônico. Entretanto, costumam não guardar adequadamente as provas eletrônicas (logs de acesso, registros de login que expiram temporariamente etc.) que comprovam o trabalho efetivo do colaborador.

grandes chances de uma das partes ajuizar ação judicial²³⁴.

Por tudo isso, a Lei n. 11.419/2006 é o marco regulatório da informatização judicial, pois abrange todas as fases/atividades para implantação do processo judicial informatizado em todo país, em todos os graus e órgãos do Poder Judiciário no Brasil²³⁵, adotando como princípio a validade de todo e qualquer ato processual realizado por meio eletrônico: *“Art. 11. Os documentos produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário, na forma estabelecida nesta Lei, serão considerados originais para todos os efeitos legais”*.

Mesmo no âmbito da Administração Pública, temos já a digitalização do processo do Tribunal de Contas da União, iniciado pela PORTARIA-TCU n. 189/2007 que aprova a realização do Projeto Processo Eletrônico Administrativo — Segedam Sem Papel e designa seu gestor.

Vazamento de dados sigilosos da empresa.	Os tribunais têm compreendido o vazamento de dados sensíveis como má conduta do colaborador, desde que comprovada pela empresa. Volta-se à necessidade, ainda, de comprovar que o colaborador possui ciência de que aquela informação é sensível.	A sociedade está voltando-se para a necessidade de políticas, normas de classificação da informação, monitoramento da rede e controles físicos de entrada e saída de pessoas, vez que uma pessoa portando um simples pen drive pode roubar dados valiosos da empresa.
Uso da imagem do colaborador.	Os tribunais têm entendido que o uso comercial e não autorizado da imagem do empregado deve ser indenizado, já que o uso da imagem não se insere nas atividades ordinárias do empregado (art. 456 da CLT).	As empresas só devem fazer uso da imagem do colaborador quando devidamente autorizadas. O termo de autorização deve ser armazenado pela empresa.

234. “RITO SUMARÍSSIMO. RECURSO ORDINÁRIO. JUSTA CAUSA. ART. 482, ‘b’, DA CLT. Burla de regras da empresa para acesso a sítios, o que era vedado. Norma regulamentar da qual o reclamante tinha conhecimento prévio. Computador e Internet, instrumentos de trabalho utilizados irregularmente, para uso pessoal. Incontinência de conduta e mau procedimento. Falta grave que está caracterizada.” (TRT2, RO 01875200843102004, Relator Carlos Francisco Berardo, j. 17-2-2009).

235. e-STF — Mais uma fase do processo eletrônico <http://www.migalhas.com.br/mostra_noticia.asp?cod=96584>.

Resolução do STF regulamenta o meio eletrônico de tramitação de processos judiciais.

Uma nova Resolução do STF publicada no final de outubro de 2009 trouxe mais avanços à tramitação eletrônica dos processos na Corte. Trata-se da Resolução n. 417/2009 (que em seu art. 21 prevê que a partir do dia 31 de janeiro de 2010 todos os atos e peças referentes às classes processuais previstas nesta Resolução somente poderão ser recebidos por meio eletrônico. A medida possibilitará agilizar o trâmite, uma vez que não será necessário deixar o escritório para protocolar a petição e não há a exigência da apresentação dos originais. Além disso, as informações relativas à transmissão, bem como os documentos transmitidos, ficam registrados em banco de dados. O novo mecanismo também possibilita a consulta por mais de um usuário ao mesmo tempo, evitando-se a vista dos autos, que contribui para a lentidão. Tribunais Associados — estão habilitados TST; TRF da 1ª Região; TRF da 2ª Região; TRF da 4ª Região; TRF da 5ª Região; TJ/ES; TJ/GO; TJ/PE; TJ/RJ; TJ/SE; TJ/AC; TJ/CE e TJ/PR (entrevista Min. Gilmar Mendes).

Destacamos que há dois modelos para determinar autenticidade dos atos processuais eletrônicos — o uso de um certificado digital da ICP-Brasil²³⁶ ou o uso de uma senha de usuário previamente cadastrada junto ao Tribunal (o que tem sido exigido que ocorra presencialmente em um primeiro momento para verificação de identidade e documentos).

Estamos preparados para isso? Ou vamos insistir em imprimir *e-mails* para guardar em arquivos de papel e depois ter de digitalizar para juntar em um processo judicial eletrônico? Não seria melhor já guardar tudo diretamente de forma eletrônica? Mas para isso precisamos de uma boa solução de Gestão Eletrônica de Documentos (GED)²³⁷ e de Arquivos de *e-mails*, para não apenas guardar, mas conseguir encontrar.

São muitos os desafios da Justiça Digital, assim como muitos são os benefícios. Por certo, conseguiremos ter ações judiciais mais céleres, visto que a eliminação do papel também diminui a burocracia. No entanto, devemos preocupar-nos com a capacidade do ambiente de processo eletrônico do judiciário:

- garantir a autenticidade (autoria das partes e dos procuradores);
- garantir o segredo de justiça (quando aplicável — acesso restrito mesmo pela via eletrônica);

236. Decisões judiciais sobre questão da autenticidade pela via eletrônica:

Ementa: “*CERCEAMENTO DE DEFESA. CONTRARRAZÕES ENVIADAS POR E-MAIL SEM CERTIFICAÇÃO DIGITAL. NÃO CONHECIMENTO. Uma vez delimitado na decisão recorrida ter sido utilizado o sistema e-doc de peticionamento eletrônico para o envio das contrarrazões ao recurso ordinário, sem a necessária certificação digital, tal como requerida na Instrução Normativa n. 3/2006 do eg. Tribunal Regional, que regula esse sistema integrado de protocolo de documentos eletrônicos (...) Recurso de revista não conhecido no tema*”. (TST, RR — 365/2007-148-03-00.0, Relator Ministro: Aloysio Corrêa da Veiga, j. 26-8-2009, 6ª Turma, Data de Publicação: 4-9-2009).

Ementa: “*AGRAVO DE INSTRUMENTO. RECURSO DE REVISTA. IRREGULARIDADE DE REPRESENTAÇÃO. (...) A tese da Recorrente de que o substabelecimento foi digitalizado por meio de escaneamento, contendo assinatura digitalizada, não lhe assiste, pois, da análise dos autos, verifica-se que a referida assinatura não lhe confere a indispensável certificação digital que decorreria da utilização de chaves criptografadas, o que seria possível pelo atendimento do disposto na Instrução Normativa 28/2005 desta Corte. Agravo de Instrumento a que se nega provimento*”. (TST, AIRR — 740/2006-491-05-40.1, Relator Ministro: José Simpliciano Fontes de F. Fernandes, j. 17-6-2009, 2ª Turma, Data de Publicação: 31-7-2009).

237. A Instrução Normativa n. 30, de 2007, do Tribunal Superior do Trabalho, quanto aos documentos eletrônicos, sejam eles originalmente eletrônicos ou digitalizados, em seu art. 25 ratifica as disposições inseridas pela Lei n. 11.419/2006 no Código de Processo Civil, nos incisos V e VI, §§ 1º e 2º, do art. 365.

- garantir integridade por meio de segurança da informação (para evitar adulteração de dados nos sistemas, mudança de sentença, voto, outros);
- criar cultura nos operadores do direito.

Estamos a caminho de uma sociedade sem papel, mas não sem documentos, como já previsto pelo próprio Código de Processo Civil brasileiro, documento é um escrito capaz de ter compreensão humana, independentemente de qual suporte esteja (pode ser papel, tecido, parede, *hard disk*, outros). A sociedade digital está muito melhor documentada, com mais controles, com mais transparência, só precisamos agora quebrar o paradigma cultural e atualizar nossos usos e costumes para atender a toda esta nova realidade empresarial e governamental. Estas normas já estão em vigor, sua empresa está preparada? Já está em conformidade? Os prazos já estão correndo.

O Poder Judiciário brasileiro, em matéria de Direito Processual Civil, já se preparou para a mudança com o advento do novo Código de Processo Civil, que tramita atualmente no Congresso Nacional pelo PL n. 166/2010, e adotou o processo eletrônico (para a comunicação de seus atos, realização de audiências, recebimento de documentos, provas eletrônicas etc.), todavia, não em sua plenitude, pois ainda continuarão a existir processos físicos. Uma das formas para se garantir o princípio da celeridade processual é a adoção do processo eletrônico, e o novo Código dá ênfase para que este seja utilizado.

8.32. Saúde Digital — Prontuário Eletrônico

Se o Fisco e o Judiciário estão ficando cada vez mais digitais, agora é a vez da saúde. A discussão sobre questões que envolvem Prontuário Eletrônico (migrar do PPS — Prontuário Pessoal da Saúde para o PEP — Prontuário Eletrônico do Paciente no Brasil e *PHR* — *Personal Health Records* nos EUA), diagnóstico por imagem, uso de biometria para identificação de pacientes junto a operadores da saúde (em substituição a carteirinha do plano), criação de um banco de dados único da Saúde, digitalização de documentos e eliminação do papel para liberar leitos em hospitais. Quais os aspectos legais a ser observados em meio a toda esta transformação e será que os profissionais da saúde estão preparados?

A saúde no Brasil é tradicionalmente descentralizada, com múltiplos agentes, bem como baseada em documentação em papel. No entanto, cada

vez mais, percebemos o quanto o uso de Tecnologia da Informação na saúde, bem como informações eletrônicas, aumenta o nível de segurança, diminui as fraudes, bem como permite acessibilidade ao próprio sistema, reduzindo burocracia, e por sua vez, o tempo de atendimento, em última análise, aumentando receita e padrão de qualidade o que beneficia a todos. O Conselho Regional de Medicina de Santa Catarina (CREMESC) manifestou-se a respeito desde 1997, sobre o uso de tecnologia para que o médico possa cumprir as exigências legais (Consulta n. 450/97 sobre o Parecer CFM n. 14/93).

Desde sempre o direito aos dados do prontuário médico é do paciente, e só cabe a ele, inclusive. No entanto, a geração do prontuário é de obrigação do médico e a guarda acaba sendo dos agentes de saúde, especialmente clínicas e hospitais, onde estes médicos atuam e consultam. Mas é só um paciente ou um familiar necessitar de suas informações para iniciar uma disputa muitas vezes jurídica, visto que há toda uma questão de sigilo médico envolvido.

Outro aspecto diz respeito à privacidade. Os dados de saúde de um indivíduo são extremamente sigilosos e sensíveis, visto o grau de impacto que podem gerar. Como as informações em um banco de dados único serão utilizadas? Afinal, há interesses divergentes. Enquanto um paciente quer que saibam o que ele possui de histórico para ser melhor atendido em uma emergência, do outro lado, uma área de Recursos Humanos de uma empresa pode querer saber se há doença preexistente e/ou não declarada pelo colaborador para decidir por sua contratação ou não, promoção ou não. Já para um plano de saúde pode representar a verificação da veracidade da declaração de saúde de um novo solicitante do plano, determinando se o contratante será aceito ou recusado, enquanto para o sistema de saúde pode representar prevenção e campanhas dirigidas para melhoria da saúde em geral.

Estas questões são reguladas por leis (Constituição Federal de 1988, art. 5º, no tocante à intimidade, Código Penal, art. 154 sobre sigilo profissional) e por autorregulamentação de mercado, especialmente Resoluções do Conselho Federal de Medicina (Res. n. 1.605/2000, 1.638/2002, 1.821/2007), Resoluções do CREMESP (Res. n. 097/2001), Código de Ética Médica (arts. 11, 69, 70, 102 a 109), ISO IEC n. 27.799/2008, entre outros. Especialmente a Resolução n. 1.821/2007 aprova as normas técnicas sobre digitalização e uso de sistemas informatizados para uso, guarda e

manuseio dos documentos dos prontuários dos pacientes. Há duas situações a ser trabalhadas: o legado (tudo o que já foi gerado no papel e que tem de ser guardado por prazos longos de 30 anos e em muitos casos chega próximo a todo o sempre) e a partir de agora para o futuro que já seria o documento nascer eletrônico, evitando os riscos e custos de seu uso e tramitação no papel. Afinal, papel é só um tipo de suporte de documento escrito, conforme prevê o Código de Processo Civil brasileiro, arts. 154, parágrafo único, 332, 333, 334, 335, outros).

Não há dúvida dos benefícios da saúde digital, mas sim sobre a capacidade de se garantir segurança e privacidade das informações, onde cada um dos envolvidos teria de ter um nível de acesso controlado e restrito a apenas aquilo que tivesse sido autorizado. Mas caberá a quem fazer a gestão dessas identidades, bem como o monitoramento do sistema, evitando riscos de segurança da informação, e também “usuários fantasmas”. Aguarda-se definição sobre o assunto pela Agência Nacional de Saúde (ANS), que já definiu padrões no tocante a requisitos de segurança (NGS1) e troca de informação em saúde suplementar (TISS).

No tocante ao prontuário médico eletrônico, seria uma grande evolução, principalmente para não termos mais de tentar decifrar inclusive o que é escrito a mão pelos médicos. Mas isso é também um desafio para o setor de saúde, visto a necessidade de treinamento, de capacitação dos profissionais para uso do computador de modo obrigatório. Lembrando ainda que não está adstrita ao ordenamento jurídico brasileiro, visto casos de internações ou tratamentos de pacientes com plano de saúde brasileiro em outros países.

A saúde digital é inevitável, mas é essencial haver padronização, que haja homologação do sistema pelas instituições que regulam a saúde, bem como que se invista em capacitação. Deve-se poder ter “confiabilidade”, ou seja, que os dados inseridos no sistema sejam autênticos e íntegros, e que isso seja preservado de modo adequado. Logo, por certo, um modelo de assinatura digital, com uso de certificado ou mesmo biometria, para garantir que foi o médico que inseriu aqueles dados no sistema é essencial. Isso já foi inclusive objeto de apreciação pelo Conselho Federal de Medicina no Parecer n. 30/2002, que trata sobre o uso do certificado digital da ICP/Brasil.

Do outro lado, o paciente também deve receber uma senha e ter o ônus de sua guarda segura, bem como poder inserir dados mas sem alterá-los. Ou seja, o sistema deve ser preparado para não sobrescrever informações, já que o

histórico em si, a evolução, a mudança das informações, fazem parte do próprio diagnóstico e são essenciais para compreensão de cada caso. A rastreabilidade da informação é uma garantia necessária ao próprio sistema, que deve ser feito de modo a permitir ser auditável.

Devemos acompanhar o Projeto de Lei PLS n. 474/2008, que altera a Lei n. 8.080/90, para dispor sobre a informatização dos serviços de saúde, em seu art. 38-A determina que *“o uso de meio eletrônico em prontuário de paciente, assim como no registro, na comunicação, na transmissão e na autorização de procedimento ambulatorial e hospitalar, de internação hospitalar, de resultado e laudo de exame, de receita médica e das demais informações de saúde serão admitidos nos termos desta Lei”*.

Mister se faz rever os processos baseados em “usos e costumes” que não possuem qualquer respaldo ou exigência legal. E que a saúde acompanhe a evolução digital da sociedade da informação, tomando o máximo proveito disso.

8.33. E-Learning

O Ensino pela Internet, ou *e-Learning*, como é mais conhecido, é, atualmente, um desafio. Desafio por ter de incorporar as novas tecnologias, o *e-mail*, os *“Chat rooms”*, a videoconferência, a multimídia junto com as características intrínsecas da Internet como acessibilidade, instantaneidade, alcance mundial e convergência para formar o mais eficiente, abrangente e ousado projeto de ensino a distância já posto em prática, sem comprometer padrão de qualidade e sem infringir os princípios éticos e educacionais que regem a relação professor-aluno, quer seja virtual, quer real.

Os cursos de ensino a distância não constituem nenhuma novidade. Em 1969, a universidade britânica Open University (www.open.ac.uk) iniciou seus trabalhos e hoje, sem ter nenhuma sala de aula, possui aproximadamente 150.000 graduados e 30.000 pós-graduados. No Brasil, em 1971²³⁸, o supletivo, destinado a suprir o rendimento escolar do ensino fundamental e médio aos jovens e adultos que não o tinham adquirido na idade apropriada, já podia, legalmen-

238. Lei n. 5.692, de 11 de agosto de 1971, antiga Lei de Diretrizes e Bases da Educação, revogada pela Lei n. 9.394, de 20 de dezembro de 1996.

te, ser ministrado através de todos os meios de comunicação disponíveis, de maneira a atingir o maior número possível de alunos. A partir da Lei de Diretrizes e Bases da Educação — LDB o ensino a distância passou a abranger todos os níveis e modalidades de ensino no Brasil.

Os cursos ministrados a distância, basicamente, podem ser divididos em cursos supletivos, de educação profissional, cursos de graduação, de pós-graduação e cursos livres. Os três primeiros estão regulamentados pelo art. 80 da Lei n. 9.394, de 1996, pelos Decretos n. 2.494²³⁹ e 2.561, ambos de 1998, e pela Portaria do Ministério da Educação n. 301, de 7 de abril de 1998. Além disso, os cursos de pós-graduação a distância já foram regulamentados²⁴⁰.

A instituição que se interessar em ministrar cursos a distância deve estar ciente de que para tal é preciso estar adequadamente credenciada. O credenciamento de instituições do sistema federal de ensino, a autorização e o reconhecimento de programas a distância de educação profissional e de graduação de qualquer sistema de ensino são de competência do Ministério da Educação e do Desporto²⁴¹.

239. De acordo com o art. 2º do Decreto n. 2.494/98, *“os cursos a distância que conferem certificado ou diploma de conclusão do ensino fundamental para jovens e adultos, do ensino médio, da educação profissional e de graduação serão oferecidos por instituições públicas ou privadas especificamente credenciadas para esse fim (...)”*. Para oferta de cursos a distância dirigidos à educação fundamental de jovens e adultos, ensino médio e educação profissional de nível técnico, o Decreto n. 2.494/98, posteriormente alterado pelo Decreto n. 2.561/98, delegou competência às autoridades integrantes dos sistemas de ensino, de que trata o art. 8º da LDB, para promover os atos de credenciamento de instituições localizadas no âmbito de suas respectivas atribuições. Assim, as propostas de cursos nesses níveis deverão ser encaminhadas ao órgão do sistema municipal ou estadual responsável pelo credenciamento de instituições e autorização de cursos — a menos que se trate de instituição vinculada ao sistema federal de ensino, quando, então, o credenciamento deverá ser feito pelo Ministério da Educação. No caso da oferta de cursos de graduação e educação profissional em nível tecnológico, a instituição interessada deve credenciar-se junto ao MEC, solicitando, para isso, a autorização de funcionamento para cada curso que pretenda oferecer.

240. A possibilidade de cursos de mestrado, doutorado e especialização a distância foi disciplinada pelo Capítulo V do Decreto n. 5.622/2005 e pela Resolução n. 1, da Câmara de Ensino Superior-CES, do Conselho Nacional de Educação-CNE, em 3 de abril de 2001. Fonte: <<http://portal.mec.gov.br/seed/index.php?option=content&task=view&id=618&Itemid=190>>.

241. Arts. 11 e 12 do Decreto-Lei n. 200, de 25 de fevereiro de 1967, e art. 11 do Decreto n. 2.494, de 10 de fevereiro de 1998. Este último foi revogado pelo Decreto n. 5.622, de 19 de dezembro de 2005.

Lembramos ainda que a falta de padrões de qualidade e a ocorrência de irregularidades de qualquer ordem podem ser objeto de diligência, sindicância e, se for o caso, de processo administrativo para apurá-los podendo até acarretar o descredenciamento da instituição.

A legislação brasileira prevê que os cursos, nas modalidades presencial ou a distância²⁴², são intercambiáveis. Isso significa que podem ocorrer transferências, nas quais os créditos e as certificações totais ou parciais obtidos em uma modalidade podem ser aproveitados em outra, o que é muito importante para proteger o consumidor-aluno de abusos e arbitrariedades que possam ser cometidas pela instituição de ensino, como cancelamento do curso, mudança de conteúdo e professores sem prévio aviso, não devolução de taxas de matrícula, entre outros.

Apesar de todas as facilidades e soluções trazidas pelas novas tecnologias, ainda existe um grande entrave à expansão dos cursos a distância, um problema para o qual ainda não se vislumbra uma saída adequada. A legislação em vigor exige (à exceção dos cursos livres) a realização de exames presenciais²⁴³, isso porque ainda não existe mecanismo eletrônico que permita um nível tal de segurança contra fraudes; mesmo as chamadas chaves criptográficas assimétricas não funcionam quando o detentor da chave privada tem interesse em que outra pessoa se passe por ele. Essa situação implica que a instituição deve estar preparada para atender em local físico todos os seus alunos, o que acaba restringindo o raio de atuação dos cursos fornecidos pela Internet.

242. A Portaria MEC n. 2.253, de 18 de outubro de 2001, autorizou até 20% da carga horária dos cursos ministrados de forma não presencial. Sendo assim, o ensino a distância e o *e-learning* tendem a superar o crescimento que vêm tendo. Mais informações podem ser obtidas no portal www.elearningbrasil.com.br. Ela foi revogada pela Portaria MEC 4.059, mas que manteve a mesma disposição.

243. Art. 7º do Decreto n. 2.494/98: "A avaliação do rendimento do aluno para fins de promoção, certificação ou diplomação realizar-se-á no processo por meio de exames presenciais, de responsabilidade da instituição credenciada para ministrar o curso, segundo procedimentos e critérios definidos no projeto autorizado". O Decreto foi revogado pelo Decreto n. 5.622/2005 e substituído pelo seguinte texto, previsto no art. 4º: "*A avaliação do desempenho do estudante para fins de promoção, conclusão de estudos e obtenção de diplomas ou certificados dar-se-á no processo, mediante: I — cumprimento das atividades programadas; e II — realização de exames presenciais. § 1º Os exames citados no inciso II serão elaborados pela própria instituição de ensino credenciada, segundo procedimentos e critérios definidos no projeto pedagógico do curso ou programa. § 2º Os resultados dos exames citados no inciso II deverão prevalecer sobre os demais resultados obtidos em quaisquer outras formas de avaliação a distância.*"

A validade dos diplomas e certificados conferidos por instituições autorizadas é nacional; certificados conferidos por instituições estrangeiras terão de ser revalidados. Da mesma forma, terão de ser revalidados em outros países (se assim a legislação local o dispuser) os certificados conferidos por instituições brasileiras a alunos residentes fora do País.

O *e-learning* vem se desenvolvendo muito, sobretudo no ensino superior e cursos livres de atualização. No Brasil, o pioneiro na graduação a distância foi o Cederj — Centro Universitário de Educação a Distância do Estado do Rio de Janeiro (www.cederj.edu.br).

Apesar de atualmente todos os níveis de ensino já serem passíveis de ser lecionados a distância, o grande filão do mercado é, sem dúvida, o dos cursos de graduação, pós-graduação e os cursos livres. Quanto aos cursos de ensino fundamental e médio, não se demonstrou ainda interesse em ministrá-los, e talvez a explicação esteja nas palavras de Robin Mason, uma das maiores especialistas mundiais em ensino a distância. Segundo ela, os estudantes na faixa etária dos 18 aos 22 anos, por exemplo, precisam do curso *face to face*, porque, nessa fase, os alunos são empurrados ao estudo pelos pais e precisam ser monitorados.

Um dos negócios mais promissores atualmente é o *e-learning* corporativo²⁴⁴. As empresas e os profissionais começaram a entender que na sociedade digital as técnicas de produção estão em constante processo evolutivo, e o ensino através da Internet tem demonstrado ser uma maneira muito eficiente de manter os funcionários constantemente atualizados por meio de cursos oferecidos pelas empresas. Aliado à vantagem da flexibilidade do ensino a distância, funcionários e empresas têm ganhado muito com as parcerias com instituições de ensino a distância.

Por tudo isso, entendemos que o *e-learning* veio para ficar e será uma ferramenta poderosa para o fortalecimento da cultura e do nível educacional de profissionais e alunos brasileiros diante do mercado globalizado, internacional e competitivo característico da sociedade digital.

244. Neste sentido há o artigo publicado na *Gazeta Mercantil* de 24 de janeiro de 2002, intitulado "Conquistas do e-Learning", de autoria de Fernando Boldrini e Reinhard Ziegler.

8.34. Aspectos legais do EAD

Cresce de importância nas instituições de ensino no Brasil o uso de métodos de educação a distância (EAD). Com isso, o modelo de sala de aula foi substituído por um professor cada vez mais digital, por uma jornada educacional com horário mais flexível. A EAD nasceu do antigo modelo de cursos por correspondência e, por certo, é um salto evolutivo no modelo de ensino, permitindo até maior acesso a sala de aula quando refletimos o seu alcance em todas as localidades do Brasil. Se um aluno ficar doente, a escola pode ir até ele.

Em vez de ter o professor em sala de aula como principal forma de apresentar a aula, o novo modelo passou a fazer uso de três figuras: o professor (quando há aula presencial), o conteudista (pessoa que desenvolve conteúdo educacional e pedagógico) e o tutor (aquele que apoia a orientação em sala de aula virtual, prestando toda assistência para os alunos por meio da Internet).

A EAD é o *e-Business* educacional. Principalmente em uma sociedade do conhecimento que demanda atualização permanente dos profissionais. Isso provocou a necessidade de elaboração de novas minutas de contratos, tanto para abranger a questão da “matrícula *online*”, dos direitos e deveres do aluno de EAD, bem como para determinar o modelo de trabalho de conteudistas e tutores, proteger direitos autorais e de imagem.

Alguns dos desafios jurídicos da EAD envolvem:

1. interação professor — aluno — limites e responsabilidades pela via eletrônica;
2. uso de redes sociais e colaboração em massa e a questão da proteção dos direitos autorais e de imagem;
3. segurança da informação dos dados dos alunos que se cadastram em portais de escolas e universidades;
4. disponibilidade do serviço e a necessidade de SLA — Acordo de Nível de Serviço;
5. portabilidade dos conteúdos — pode ou não copiar, colar, transmitir conteúdos de EAD?

O desafio em termos de novos modelos para governança no ambien-

te educacional está em como proteger adequadamente as relações jurídicas da instituição de ensino neste novo cenário, em que há uma exposição muito maior ao mesmo tempo que precisamos compartilhar conhecimento, dentro de uma conformidade legal, atendendo aos preceitos do Novo Código Civil (arts. 186, 187, 927, 932 e 1.016), já que a Diretoria pode sim responder por uma gestão que não esteja aderente às boas práticas legais.

Mesmo o modelo de contratação por hora-aula não é mais suficiente para retratar estas novas relações advindas com a EAD. Ao contratar um conteudista, por exemplo, ou até mesmo um *designer* para a criação gráfica de seu curso deve o contrato abordar cláusula específica de responsabilidade sobre as imagens e qualquer conteúdo utilizado, devendo ainda constar expressamente os meios de utilização, vez que a lei é clara quando determina que os contratos de cessão de direitos autorais serão interpretados restritivamente. O tempo de cessão também é importante, mesmo que seja para constar que será perpétuo, ou do tempo específico quando for o caso.

Portanto, a instituição de ensino deve ficar atenta a tudo que acontece nos ambientes que disponibiliza, seja ele físico ou virtual. É essencial atualizar os contratos e ter regras mais claras para este novo ambiente.

8.35. Crimes eletrônicos

Legislar sobre a matéria de crimes na era Digital é extremamente difícil e delicado. Isso porque sem a devida redação do novo tipo penal corre-se o risco de se acabar punindo o inocente. Além disso, sabemos que em computação forense as “testemunhas máquinas” não conseguem diferenciar “culpa” de “dolo”. Ou seja, um computador não traz informações de contexto da situação, tampouco consegue dizer se foi “sem querer”, sem intenção. Um exemplo disso é a tentativa de se tipificar o crime de envio de arquivo malicioso em *e-mail*. Muitas pessoas, até por excesso de inocência, enviam *e-mail* com vírus para outras. Além disso, o computador pode ter se tornado uma máquina “zumbi”, sendo usada remotamente por terceiros para gerar este tipo de ação. Por isso, devemos acompanhar esta discussão toda no Legislativo, visto que é necessária. Nós temos atualmente novas condutas, bem como condutas antigas que merecem um novo tipo de punição. Desse modo, precisamos, para a matéria de crimes eletrônicos, de uma boa atualização do Código Penal brasileiro, do Código de Processo Penal brasileiro e da Lei de Execuções Penais. Mas

nada disso será útil sem um modelo forte de prova de autoria, de uma identidade digital obrigatória²⁴⁵.

245. Ver leis sancionadas pela Presidenta Dilma Roussef, em 30-11-2012, sobre Crimes Digitais. Seguem abaixo duas tabelas resumidas com o que foi aprovado como novas condutas criminais no ordenamento jurídico brasileiro:

Lei n. 12.735 — Lei Azeredo

TIPO PENAL	ARTIGO
Equiparação de Cartão de Crédito a documento particular — idêntico ao artigo da Lei 12.737.	Art. 2º (VETADO)
Traição e favorecimento ao inimigo — Não há delimitação de dado eletrônico, ficando prejudicada a interpretação.	Art. 3º (VETADO)
Norma programática para instalação de órgãos investigativos especializados.	Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
Complemento à lei que tipifica os crimes de discriminação, elencando que os meios em que a remoção de conteúdos não permitidos pela lei podem ser removidos.	Art. 20. § 3º: II — a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

Lei 12.737 — Lei Carolina Dieckmann

TIPO PENAL	ARTIGO
Invasão de dispositivo informático.	Art. 154-A. Invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena — detenção, de 3 (três) meses a 1 (um) ano, e multa.
Produção de recursos que possibilitam a invasão.	§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no <i>caput</i> .
Causa de aumento de pena.	§ 2º Aumenta-se a pena de um sexto a um terço se a invasão resulta prejuízo econômico.
Crime qualificado.	§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena — reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
Causa de aumento de pena.	§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
	§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I — Presidente da República, governadores e prefeitos; II — Presidente do Supremo Tribunal Federal; III — Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV — dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

O crime eletrônico é, em princípio, um crime de meio²⁴⁶, isto é, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, ou seja, o crime cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por *hackers*²⁴⁷, que de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros. Isso quer dizer que o meio de materialização da conduta criminosa pode ser virtual; contudo, em certos casos, o crime não²⁴⁸.

A maioria dos crimes cometidos na rede ocorre também no mundo real. A Internet surge apenas como um facilitador, principalmente pelo anonimato

Condição de propositura da ação.	Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.
Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública — Nova redação.	Art. 266. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
Causa de aumento de pena.	§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.
Falsificação de documento particular — Complemento.	Art. 298. Falsificação de cartão Parágrafo único. Para fins do disposto no <i>caput</i> , equipara-se a documento particular o cartão de crédito ou débito.

Fonte: Patrícia Peck Pinheiro Advogados — 12-12-2012.

246. Segundo proposto por Robson Ferreira em sua tese de crimes eletrônicos, podemos estudar uma classificação dos crimes por computador levando em conta o papel do computador no ilícito: 1) quando o computador é o alvo — p. ex.: crime de invasão, contaminação por vírus, sabotagem do sistema, destruição ou modificação do conteúdo do banco de dados, furto de informação, furto de propriedade intelectual, vandalismo cibernético, acesso abusivo por funcionário, acesso abusivo por terceirizados, acesso abusivo de fora da empresa; 2) quando o computador é o instrumento para o crime — p. ex.: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores ou alterações de saldos e fraudes de telecomunicações, divulgação ou exploração de pornografia; 3) quando o computador é incidental para outro crime — ex.: crimes contra a honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, registro de atividades do crime organizado; 4) quando o crime está associado com o computador — p. ex.: pirataria de *software*, falsificações de programas, divulgação, utilização ou reprodução ilícita de dados e programas, comércio ilegal de equipamentos e programas.

247. No Brasil, a tendência de que sejam tipificadas algumas condutas criminosas próprias da Internet se confirmou com a aprovação de duas leis de crimes digitais em 2012.

248. Fortalecendo esta corrente de pensamento, temos o julgamento pelo Ministro Sepúlveda Pertence, do STF, de um *habeas corpus* (76689/PB 22-9-1998) sobre crime de computador: “Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminosa, o meio técnico empregado para realizá-la pode até ser de invenção posterior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo”.

que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal ou para o Direito Penal Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória, bem como à necessidade de tipificação penal de algumas modalidades que, em razão de suas peculiaridades, merecem ter um tipo penal próprio.

Os crimes eletrônicos ou cibernéticos têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação telefônica e de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de “*e-mail bombing*”²⁴⁹, o “*e-mail com vírus*”²⁵⁰, o “*spam*”. Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas²⁵¹.

Para o Direito Digital, IP constitui uma forma de identificação virtual. Isso significa que o anonimato na rede é relativo, assim como muitas identidades virtuais podem não ter um correspondente de identidade real. Como analogia, é o mesmo que ocorre quanto a contas e empresas fantasmas, cuja identidade física pode ser falsa. Isto na rede, devido a sua dimensão e caráter globalizado, faz com que a facilidade para “criar laranjas” seja ainda maior.

Especificamente no Brasil, os crimes²⁵² mais comuns na rede são o estelionato²⁵³ e a pornografia infantil²⁵⁴. Os *e-mails* gratuitos são outro agente de

249. “*e-mail bombing*” — envio de *e-mails* imensos ou vários *e-mails*. Causa atraso na recepção e gasto adicional com conta telefônica. Aplicável o art. 163 do Código Penal (crime de dano).

250. “*e-mail com vírus*” — envio de vírus anexado ao *e-mail*. São aplicáveis os arts. 151, § 1º, II e III, e 163 do Código Penal, com aplicação do art. 65 da LCP, com pena de prisão simples de 15 dias a 2 meses, ou multa por perturbação da tranquilidade.

251. Constituição Federal, art. 5º, XII: “*é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*”. A Lei n. 9.296, de 24 de julho de 1996, regula o inciso XII, parte final, do art. 5º da CF em seu art. 1º, parágrafo único: “*O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informação e telemática*”.

252. Os ataques pela Internet saíram definitivamente da fase de vandalismo e se tornaram uma atividade ilícita lucrativa. Hoje, o chamado cibercrime visa a resultados financeiros e se mostra como mais uma ramificação do crime organizado.

253. Código Penal brasileiro, art. 171.

254. O escopo exato do problema da pornografia infantil é difícil de determinar, embora

expansão, pois seus dados não são necessariamente comprovados. Uma prática recomendável seria obrigar os provedores a identificar suas contas ativas e inativas, utilizando uma tecnologia de fotografia do usuário, ou seja, ter a comprovação de seus dados e, se possível, sua imagem digital. Isso, associado a uma prática de cadastramento dos usuários, no mesmo procedimento adotado pelos bancos, permite que realmente existam meios de prova confiáveis, rompendo-se a maior barreira à segurança na rede.

Devemos observar que, nos provedores pagos, é mais fácil identificar os usuários e restringir práticas delituosas, porque há emissão de fatura mensal ou débito em cartão de crédito, cujos bancos de dados são normalmente mais detalhados e seguros²⁵⁵. No entanto, as contas gratuitas não possibilitam um controle tão constante.

É responsabilidade do usuário, por sua vez, operar com senhas de difícil decifração, assim como cabe ao provedor conferir-lhe um *software* de criptografia adequado e atualizado. Usar datas de nascimentos ou nomes comuns, por exemplo, torna muitas operações bancárias do mundo real inseguras — em ambiente virtual, a insegurança gerada por procedimentos desse tipo é ainda maior. Como as senhas são a assinatura eletrônica dos indivíduos na rede, decifrá-las significa aprender a falsificar uma assinatura.

Ressalte-se que, com a internet móvel, a individualização do usuário cresce, fazendo com que o celular se torne um prolongamento de sua existência

fique claro que o problema explodiu com o advento da Internet. Um estudo a respeito de leis sobre pornografia infantil em 186 países membros da Interpol ao redor do mundo produziu resultados alarmantes: mais da metade desses países (95) não possui leis adequadas relacionadas à pornografia infantil. De maneira surpreendente, apenas cinco dos países estudados possuem leis consideradas abrangentes o suficiente para ter um impacto significativo sobre o crime. Eles são: Austrália, Bélgica, França, África do Sul e Estados Unidos (http://www.icmec.org/missing-kids/servlet/PageServlet?LanguageCountry=en_X1&PageId=3085).

255. Por exemplo, se não afastar a suspeita de que a linha telefônica foi fraudada por terceiros, a operadora não pode cobrar as contas questionadas pelo usuário. O entendimento é da 1ª Vara Cível de São Paulo ao julgar uma ação da empresa Arcor do Brasil contra a Telesp, atual Telefonica. O juiz entendeu que, como a operadora não descartou a possibilidade de fraude eletrônica e não demonstrou que vem desenvolvendo algum sistema de segurança de combate a *hackers*, não há como cobrar as faturas reclamadas. Para o juiz “*somente é possível concluir pela verossimilhança das alegações do consumidor e hipossuficiência — esta aferida em função da dificuldade na realização da prova, decorrente da desigualdade quanto à detenção de conhecimentos técnicos específicos da atividade do fornecedor*”. Por isso, como a empresa de telefonia não conseguiu provar a inexistência de fraude, ela não poderá exigir o pagamento das faturas questionadas (TJSP, Proc. 583.00.1996.637886-5/000000-000, 1ª Vara Cível).

no mundo digital, a partir do qual ele pode realizar uma série de negócios eletronicamente. O roubo e o furto de celulares tornam-se comuns não apenas pelos recursos conseguidos com a venda do aparelho no mercado paralelo e pelo uso da linha para ligações ilegais — torna-se quase um sequestro, em que a identidade da pessoa proprietária do aparelho é assumida pelo praticante do roubo por determinado período de tempo. A falta de zelo gerada pela falta de tempo é um estímulo aos crimes virtuais. Por isso, grande parte da responsabilidade pelo crescimento dos crimes virtuais se deve à conduta displicente de muitos usuários.

O maior problema jurídico dos crimes virtuais é a raridade de denúncias e, pior, o despreparo da polícia investigativa e de perícia para apurá-las. Embora já seja possível fazer boletins de ocorrência pela Internet²⁵⁶, são poucas as equipes e profissionais preparados para a investigação de um crime virtual²⁵⁷. É importante lembrar que os criminosos da Internet já não são criminosos incomuns — a imagem de um sujeito extremamente inteligente e com vasto conhecimento técnico já não corresponde à realidade, pois atualmente é muito fácil encontrar na Internet o código-fonte aberto de um vírus ou trojan. Alguns criminosos praticam até mesmo a clonagem de *sites*, que, nesse caso,

256. Portaria DGP n. 1, de 4 de fevereiro de 2000: Disciplina a recepção e o registro de ocorrências policiais e denúncias por meio eletrônico. Também vale a análise do Decreto estadual/SP n. 50.386, de 22 de dezembro de 2005, o qual afirma que o atestado de antecedentes a que se refere o Decreto n. 47.574, de 8 de janeiro de 2003, poderá ser obtido por meio de acesso a sítio na Internet no portal do Governo do Estado de São Paulo.

257. O governo de São Paulo anunciou em 2001 (Fonte: <http://www.pcworld.com.br> — terça-feira, 2 de outubro de 2001 — 16h20) a criação de uma divisão da polícia para atender a crimes ainda sem legislação específica, como uso indevido da Internet, pirataria e falsificações. A Divisão de Investigações Gerais (DIG), ligada à Polícia Civil, trabalhará com quatro novas delegacias especializadas. A Delegacia de Bens Imateriais vai combater os crimes de pirataria, ou seja, todos os tipos de delitos contra a propriedade industrial, desde falsificação de roupas até cópias indevidas de *software*. A Delegacia de Crimes Contra a Fé Pública e Roubo de Medicamentos combaterá os crimes como falsificação de documentos ou assinaturas e também os roubos, furtos ou desvios de medicamentos. Já a Delegacia de Estelionatos vai retirar essa atribuição dos distritos para possibilitar a criação de um banco de dados centralizado, que permita o aumento da agilidade e eficiência no combate a esse tipo de crime. Finalmente, a divisão de Delitos Praticados por Meios Eletrônicos será especializada no combate aos crimes praticados por *hackers*, que se utilizam da Internet para desviar recursos financeiros e informações, enviar vírus de computador ou fazer ameaças via *e-mail*, entre outros. Atualmente, a DIG-DEIC — 4ª Delegacia de Repressão aos Crimes de Informática de São Paulo (SP), presta atendimento presencial, por telefone e via *Web*, estando localizada no endereço: Av. Zacki Narchi, 152, Carandiru — São Paulo (SP), Fone: (11) 6221-7011 ou 6221-7030, *e-mail*: 4dp.dig.deic@policiacivil.sp.gov.br.

exige *expertise* tecnológica acima da média, utilizando-os para roubar informações dos usuários, tais como RG, CPF, residência, telefone, *e-mail*, dados bancários — informações utilizadas posteriormente para que o criminoso assuma outras identidades em operações comerciais com uso de cartão de crédito clonado. O combate a esses crimes torna-se extremamente difícil por dois motivos: a) a falta de conhecimento do usuário, que, dessa forma, não passa às autoridades informações relevantes e precisas; e b) a falta de recursos em geral das autoridades policiais.

A maioria das investigações sobre crimes virtuais exige quebra de sigilo²⁵⁸. Isso porque, como vimos no capítulo sobre segurança, a testemunha do crime é aquele que detém os protocolos IP, aquele que armazena os dados sobre as transações ocorridas eletronicamente. Da mesma forma, as provas eletrônicas — que muitos hesitam em aceitar juridicamente, alegando que são altamente adulteráveis — podem passar por perícia técnica rigorosa para serem aceitas em processos. Como já afirmamos, com profundo conhecimento da tecnologia, é possível ter provas virtuais muito mais confiáveis que as do mundo real.

O Direito Digital traz a obrigação de atualização tecnológica não só para advogados e juízes, como para delegados, procuradores, investigadores, peritos e todos os demais participantes do processo. Tal mudança de postura é necessária para que possamos ter uma sociedade digital segura; caso contrário, coloca-se em risco o próprio ordenamento jurídico.

O maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente marginal, um submundo em que a ilegalidade impera. Essa postura existe porque a sociedade não sente que o meio é suficientemente vigiado e que seus crimes são adequadamente punidos. O conjunto norma-

258. Os registros dos usuários conectados à rede, mantidos por seus provedores, gozam de proteção e só podem ser requeridos pela autoridade judicial competente. Nesse sentido temos a liminar concedida pelo Juiz José Ricardo Machado, da 1ª Vara da Fazenda Pública Municipal de Goiânia, determinando que o provedor de serviços de acesso à Internet terá de quebrar o sigilo de cadastro de um de seus clientes para que ele possa ser identificado. Na ação, a Procuradoria-Geral do Município relata que, no dia 26 de janeiro de 2001, um cliente do UOL, com endereço eletrônico tacl@uol.com.br, transmitiu uma mensagem na qual divulgou a notícia, tida como falsa pela Administração Pública. Recentemente, o STF foi acionado em função de um processo contra um jovem acusado de pedofilia. Após a promotoria requisitar (e obter) ao provedor de acesso conversas que comprometiam o acusado em salas de bate-papo, o réu, alegando quebra de sigilo das comunicações, recorreu. O STF não acatou o recurso, considerando que, como o ambiente virtual é informal, ele está fora do alcance da lei de sigilo e proteção à privacidade.

-sanção é tão necessário no mundo digital quanto no real. Se houver essa falta de crédito na capacidade punitiva da sociedade digital, os crimes aumentarão e os negócios virtuais serão desestimulados.

Muitas pessoas que não cometem crimes no mundo real por medo de serem pegos, acabam, de algum modo, interessando-se pela prática delituosa virtual. É o caso, por exemplo, do grande número de adolescentes de classe média, que praticam atos ilegais na rede e sentem-se bastante seguros em fazê-lo. Esse tipo de crime tem um traço cultural que se aproxima do vandalismo.

Os *hackers*, pessoas que conseguem invadir sistemas de empresas e outros sistemas conectados à rede — uma modalidade criminosa criada com o surgimento de redes eletrônicas e não da Internet, visto que já existiam invasões a sistemas antes mesmo da Internet —, podem ser divididos em duas categorias: a dos “Heróis” e a dos “Mercenários”.

Os “Heróis” são os *hackers* que cometem o crime buscando tornarem-se ídolos em sua coletividade, como os pichadores de muros, admirados por grupos adolescentes da região. Essa postura cultural é difícil de combater, mas pode ser desestimulada pela ideia de que será descoberta e punida — com punições como a prestação de serviços comunitários em locais públicos²⁵⁹, de modo a envergonhá-los diante de seus pares.

Já os “Mercenários” são os *hackers* profissionais, cuja origem remonta às grandes corporações privadas e aos órgãos de espionagem governamental. Seu aprimoramento é financiado pela espionagem entre países e pela espionagem industrial, como um meio para o roubo de informações secretas. São responsáveis também pelos grandes investimentos feitos pelas corporações em sua própria segurança, o item mais caro dentro da categoria de tecnologia nas empresas, e pelos custos gerados por sua constante necessidade de atualização.

Como num velho filme de faroeste, em que os pistoleiros mais rápidos daquelas terras onde inicialmente não existia a lei acabavam sendo contratados pelas comunidades que ali queriam estabelecer-se para se tornarem seus xerifes,

259. Para exemplificar, temos o caso do hacker canadense que usava o nick name de Jon o jOn, considerado culpado de haver ingressado ilegalmente nos sistemas de computação de várias instituições estrangeiras, entre as quais se encontram a NASA, a Universidade de Harvard, entre outras. A sentença aplicada a este jovem surpreendeu muita gente: 240 horas de trabalho comunitário, liberdade condicional por um ano, uso restrito de computadores e a obrigação de dar aulas em um colégio local sobre os malefícios causados pelos hackers. (Fonte: LEGALES 20-6-2000.) Em 24 de junho de 2011, *hackers* tiraram do ar diversos sites do governo brasileiro, preocupando a área de Segurança da Informação quanto a vazamento de informações relacionadas ao governo, e se os supostos invasores tiveram acesso a tais informações (Fonte: TV Cultura, 25-6-2011).

grandes *hackers* são contratados por corporações e governos para prestarem serviços. Mas é importante ressaltar que a prestação de serviço, desde que não ilegal, não é crime. O crime se configura na invasão não autorizada, no furto de informações confidenciais, no acesso não permitido, independentemente do uso de senha autorizada²⁶⁰. A punição mais adequada para esse tipo de criminoso é a pecuniária, associada a prestação de serviços comunitários em áreas de inteligência governamental ou na ajuda para investigação e descoberta de outros *hackers*, em colaboração com a polícia. Colocá-lo simplesmente na cadeia junto a criminosos comuns é uma irresponsabilidade pública, já que pode provocar a criação de uma geração de supercriminosos, o que é muito pior — mais ou menos o que ocorreu quando a ditadura brasileira colocou prisioneiros políticos junto com criminosos comuns (muitas pessoas consideram que essa prática gerou o crescimento do crime organizado no País — traficantes de droga, por exemplo, aprenderam a estrutura política dos grupos clandestinos, aplicando-a às suas próprias organizações).

Questão curiosa é a que surge com o uso dos meios eletrônicos pelas corporações criminosas²⁶¹, já que é um meio efetivo para baixar custos, otimizar decisões e dar logística não apenas para as empresas do mundo legal, mas também para as empresas do mundo ilegal. A máfia, por exemplo, foi uma das

260. Conforme a Lei n. 9.983/2000, que altera o Código Penal, em especial o art. 313-A: “Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena — reclusão, de 2 (dois) a 12 (doze) anos, e multa”.

261. Um dos maiores problemas trazidos pelo anonimato na rede, talvez, é a capacidade que ela oferece de servir como suporte de organizações criminosas: A Internet, assim como outras redes informatizadas, traria vantagens de acessibilidade remota, logística e instantaneidade (características tão atraentes para o comércio eletrônico) a serviço de grupos terroristas, mafiosos, redes de prostituição e pedofilia e tráfico de drogas e de armas. O desafio dos governos é conciliar a proteção à privacidade (que conta com grande número de grupos não governamentais, principalmente na Europa) com a necessidade de, efetivamente, ter uma vigilância dentro da Internet capaz de coibir a prática de atos ilícitos. Em nome da segurança e da guerra ao terror, o governo dos EUA investe contra os direitos individuais. Criado em outubro de 2001 pelo Presidente George W. Bush, o *USA Patriotic Act* visa a facilitar a captura de terroristas e, para tanto, permite aos órgãos de segurança e de inteligência vasculhar a privacidade dos cidadãos. Literalmente, *Patriotic Act* significa “lei patriótica”, mas é também a abreviação de “*Provide Appropriate Tools Required to Intercept and Obstruct Terrorism*” (prover ferramentas necessárias para interceptar e obstruir atos de terrorismo). Livre de ordenação judicial, essa nova lei assegura aos agentes poder para rastrear e-mails, vigiar o uso da Internet e grampear ligações telefônicas. Obriga bibliotecas e livrarias a informar que livros buscaram determinados cidadãos e permite a detenção de “suspeitos” por períodos prolongados. (Fonte: *Folha de S. Paulo*, 2 out. 2003). Outros regramentos, como o *Foreign Intelligence Surveil-lance Act*, de 1978, também são aplicados na luta contra o terrorismo.

primeiras organizações a perceber o imenso potencial das transações eletrônicas para a lavagem de dinheiro. Cartéis de tráfico de drogas usam as facilidades da rede para fechar negócios bilionários, assim como grupos terroristas já praticam o que se chama “Ciberterrorismo”.

Em meados de 2011, presenciamos vários ataques de negação de serviço a *sites* do governo brasileiro que ficaram instáveis até sair do ar. Com isso, voltou à tona no Congresso Nacional o trâmite do Projeto de Lei n. 84/99, que foi aprovado com alguns artigos vetados, em 30-11-2012. Assim, o Poder Público precisa estar mais atento às questões de segurança da informação nacional. Os ataques são possíveis porque encontraram vulnerabilidades e também pela falta ou precariedade na estratégia de um plano de contingência e continuidade, tendo em vista que, no início, estes *sites* eram apenas institucionais. O Poder Legislativo brasileiro está se movendo para ter alguma punição no futuro?

Os Projetos de Lei n. 2.793/2011 e n. 84/99 foram sancionados e promulgados pela Presidência da República em 30-11-2012. O PL n. 2.793/2011 foi apresentado como proposta alternativa ao n. 84/99. Os tipos penais da principal característica do crime foram aprovados nesse projeto com a inclusão do art. 154-A no Código Penal Brasileiro.

Isso por certo foi um avanço, visto que já se discutia por tantos anos uma lei mais específica para crimes digitais; no entanto, do ponto de vista de amadurecimento do Ordenamento Jurídico, há 3 estágios evolutivos para que um país dê tratamento adequado às novas questões criminais, em especial no tocante à segurança pública digital:

- 1º Estágio — ter lei penal que trate os novos delitos e condutas ilícitas que ocorrem no ambiente da *web* — alcançado pelo Brasil em 2012 mesmo que de modo inicial (poucos artigos foram aprovados).

- 2º Estágio — garantir a capacidade de guarda de prova de autoria para a penalização do infrator — o que o Brasil ainda está discutindo no âmbito do Marco Civil da Internet.

- 3º Estágio — criar um modelo próprio de cárcere digital para colocar o criminoso versão 2.0, evitando que haja apenas cárcere físico e ele continue, mesmo que preso, a agir por meio da *web*, bem como investir em sua reintegração na sociedade no combate ao próprio crime digital — isso o Brasil nem iniciou, pois exigiria a revisão de todo o modelo de execuções penais e penitenciário, como outros países já estão fazendo, em especial EUA e Comunidade Europeia.

Logo, o Brasil entrou recentemente no 1º estágio, visto que a Lei n. 12.737, de 30 de novembro de 2012, conhecida como projeto Carolina Dieckmann, foi

sancionada sem vetos. Nessa norma, é tipificado o uso de dados de cartões de crédito ou débito obtidos de forma indevida ou sem autorização. A lei equipara essa prática ao crime de falsificação de documento particular, sujeito à reclusão de 1 a 5 anos e multa. Além disso, criminaliza a invasão de dispositivos eletrônicos alheios que estejam ou não conectados à internet — como celulares, *notebooks*, *desktops*, *tablets* ou caixas eletrônicos — para obter ou adulterar dados no sistema e conseguir uma vantagem ilícita. A pena prevista para o crime é de 3 meses a 1 ano de prisão, além de multa. Receberá a mesma pena quem produzir, oferecer ou vender programas de computadores que permitam a invasão, como os vírus de internet. Já quem obtiver informações sigilosas ou violar comunicações eletrônicas privadas ou segredos comerciais, como senhas ou conteúdos de *e-mails*, pode receber de 6 meses a 2 anos de prisão. A pena aumenta de 1/3 a 2/3 se houver divulgação ou comercialização dos dados obtidos. Outra mudança é a criminalização da interrupção intencional do serviço de internet, normalmente cometida por *hackers*. A pena estipulada no projeto é de 1 a 3 anos de detenção, além de multa.

Infelizmente, apesar do grande passo que foi dado, muitos tipos penais novos, puramente digitais, não foram aprovados, pois estavam no Projeto de Lei Azeredo. Isso vai na contramão internacional, visto que muitos países já têm discutido o limite que distingue a prática de um crime eletrônico comum e quando ele se torna um ato de cyberterrorismo ou de guerra cibernética, já que o ataque intencional a *site* de governo com objetivo de retirar do ar e furtar dados é considerado de altíssima gravidade.

Portanto, a adequada vigilância da Internet pela polícia e pelo Poder Judiciário, bem como de todas as tecnologias digitais e convergentes existentes ou a serem inventadas, permite uma ferramenta poderosa para a descoberta de redes criminosas que atuam no mundo real, mas se comunicam virtualmente.

É importante ressaltar que não há somente grandes crimes na Internet. Há outros crimes mais corriqueiros que todos os usuários correm o risco de cometer sem se dar conta. Informações caluniosas distribuídas por *e-mail* são exemplos claros. Um usuário pode recebê-las em sua caixa postal e, ao reenviá-las, acabar corroborando a calúnia. Claro que se pode recorrer ao excludente de responsabilidade, mas é importante saber que, ao enviar um *e-mail*, o usuário está procedendo de modo muito mais responsável do que quando apenas envia uma carta, já que o *e-mail*, mais que carta, é um veículo de publicidade online, ou seja, dependendo do número de receptores, é como se fosse uma mídia; sendo assim, está inclusive submetido à Lei de Imprensa. É natural que,

conforme as condutas humanas evoluem e se sofisticam, também a legislação criminal deve ser atualizada e aprimorada. Recentemente o Ordenamento Jurídico Brasileiro obteve uma grande conquista, com a publicação da Lei n. 11.829, de 25-11-2008. Conforme o novo art. 241-A, § 1º, I e II, e § 2º, se a empresa ou órgão público disponibiliza acesso à Internet ou dispositivos móveis de armazenamento aos seus colaboradores/funcionários, e, por conta disso, é encontrado material pedófilo em seus computadores e a instituição se omite perante tal situação, ela poderá ser responsabilizada criminalmente, o que se dará na pessoa do responsável legal pela prestação do serviço. Logo, se o departamento de TI é responsável pela liberação de acessos e monitoramento de conteúdo na rede da empresa ou órgão público, está ciente dessa ocorrência e não comunica o departamento responsável (Jurídico, Comitê de Segurança da Informação), consequentemente o gerente de TI (ou outro superior da área) poderá ser responsabilizado criminalmente por tais condutas (art. 241-A, § 2º). Obviamente que, até a efetiva prisão, ocorrerá o seu indiciamento, e se restar provado pela perícia durante o Inquérito Policial ou Processo Penal que a responsabilidade pelo conteúdo é única e exclusivamente de outro colaborador, e que o gerente de TI não foi omissor para denunciar o fato a autoridade, ele poderá sair ileso, sendo então punido o legítimo proprietário do conteúdo.

A inovação jurídica está em se responsabilizar quem armazena, o que de certo modo se aproxima muito com o ilícito relacionado ao tráfico de entorpecentes. Desse modo, se a empresa ou instituição pública, ao tomar ciência da existência desse tipo de material em seus computadores, comunicar às autoridades competentes sobre a prática do crime de pedofilia, não será responsabilizada pela armazenagem do material (exclusão de ilicitude), conforme dispõe o art. 241-B, § 2º²⁶².

262. A Lei n. 11.829/2008 alterou a redação dos arts. 240 e 241 do Estatuto da Criança e do Adolescente (Lei n. 8.069/90), o que mostra um grande avanço no combate ao crime de Pedofilia no Brasil, visto que a "armazenagem" do conteúdo passa a configurar o crime também, conforme nova redação abaixo:

"Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive através de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena — reclusão, de 3 (três) a 6 (seis) anos, e multa.

§ 1º Nas mesmas penas incorre quem:

I — assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o *caput* deste artigo;

Também são corriqueiros os *sites* de protesto, que surgem para expor indignação contra determinada pessoa, empresa ou governo. É importante ficar atento aos limites desse tipo de *site*: posso expor restrições de gosto pessoal a determinado alvo, mas, no momento em que passo informações sobre ele, terei de prová-las verdadeiras, sob pena de estar cometendo crime.

Além da questão da prova, como vimos, a questão da territorialidade no âmbito de crimes digitais é a que mais gera controvérsias. O Direito Criminal está, sempre, submetido a determinado território nacional²⁶³ — o que extrapola esse território está sujeito à existência ou não de acordos entre os países envolvidos. Uma investigação bem-feita pode não chegar à punição do crime e execução da pena, se for detectado que o criminoso opera de outro país e não for conseguida a extradição dele ou seu julgamento no país de origem. Já ocorrem movimentos entre as diversas diplomacias para que se estabeleçam regras internacionais²⁶⁴ de punição a crimes pela Internet. A procedência do ato criminoso será mais bem resolvida quando se aprimorarem os mecanismos de

II — assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o *caput* deste artigo.

§ 2º As condutas tipificadas nos incisos I e II do § 1º são puníveis quando o responsável legal pela prestação do serviço, regularmente comunicado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o *caput* deste artigo.

Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

(...)

§ 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:

I — agente público no exercício de suas funções;

II — membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;

III — representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário".

Para acompanhar os demais projetos de lei de crimes eletrônicos acessar o *site* <<http://www.senado.gov.br/sf/atividade/materia/push/>> ou se cadastrar em nossa *newsletter* mensal que traz o monitoramento legislativo em <www.pppadvogados.com.br>.

263. O art. 6º do Código Penal, que determina o lugar do crime, reza o seguinte: "Considera-se praticado o crime no lugar em que ocorreu a ação ou a omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado".

264. Para o estudo deste tema é importante a leitura sobre a Convenção de Budapeste.

identificação dos usuários. Mas este tema é extremamente polêmico. A tendência mundial é a definição de um padrão de identidade digital obrigatória, mas isso gera um conflito direto com a “cultura do anonimato” que a Internet trouxe, de certa forma.

Tendo em vista que as pessoas, as empresas e a própria riqueza da sociedade está migrando para o ambiente virtual, é natural que o crime também. Neste sentido, o estudo desta disciplina é essencial para o profissional do direito, visto que cada vez mais será demandado a ele compreender as questões relacionadas a prática de ilícitos em ambientes eletrônicos²⁶⁵.

Os incidentes mais comuns no ambiente digital envolvem contaminação por vírus, uso indevido ou não autorizado de senha (qualquer tipo, do *e-mail* pessoal a do Internet *banking*), uso indevido de número de cartão de crédito, furto de dados, fraude, falsa identidade ou falsidade ideológica (alguém se passar por outra pessoa), ofensas digitais (em geral tipificadas como crimes contra a honra — difamação, calúnia e injúria, mas tem também a ameaça e a contravenção penal de perturbação da paz do indivíduo que ocorre com *cyberbullying* em geral). Ele também pode ser envolvido em uso não autorizado de imagem (seja a dele ou ele fazendo uso da de outra pessoa), infração de direitos autorais (pirataria e plágio), dano em geral, espionagem eletrônica e todo tipo de vingança digital que pode envolver até apagamento dos seus dados, alteração do seu perfil, sequestro de domínio (em especial no caso das empresas).

A informação postada em uma comunidade virtual, inclusive uma foto, torna-se uma informação de acesso mais fácil, pois está publicada. A Constituição Federal de 1988, em seu art. 5º, X, bem como o Código Civil nos arts. 20 e 23 protegem a imagem da pessoa. Logo, não é porque uma pessoa publicou sua foto em uma comunidade que dá o direito a alguém pegá-la e colocá-la em outro lugar. Há necessidade de autorização prévia e expressa para uso de imagem. Mas há sim o risco de alguém vir a fazer isso, bem como adulterar a foto, mudá-la, editá-la, mudar o contexto (colocar inserida em outra temática que possa denegrir a imagem do fotografado), além de ela poder ser usada para identificação da pessoa e até mesmo atrair eventual situação de sequestro. Logo, deve-se evitar exposição demasiada de imagem na *web*. Ainda mais de fotos que a pessoa possa se arrependar ou que possam dar uma conotação

265. Para aprofundar no estudo do tema, recomendo a leitura dos artigos de uma jovem e brilhante advogada criminalista, Dra. Gisele Truzzi, <<http://www.truzzi.com.br/artigos.htm>> e <<http://www.pppadvogados.com.br/conhecimento.asp?Passo=Exibir&Materia=433>>.

distinta da que ela gostaria. Ex.: um executivo ter uma foto particular publicada por ele ou seus familiares e o que está retratado na imagem não ser condizente com o cargo dele e isso poder vir a prejudicá-lo.

Pela minha experiência, grandes empresas estão mais expostas, portanto, são alvos mais fáceis. Quanto mais famosa e conhecida uma marca, mais incidentes ela está sujeita a passar na Internet no tocante a uso não autorizado de marca, abuso de liberdade de expressão por terceiros, registro indevido de domínio ou similar a domínio existente para fins de *cybersquatting*, uso da marca em *e-mails* falsos para ludibriar pessoas a passarem dados e a se contaminarem por arquivos maliciosos.

No Brasil, como em outros países, o ordenamento jurídico passa por permanente atualização provocada pela própria mudança e evolução da sociedade. Surgem novos casos, novas condutas, novos valores e isso provoca um dinamismo natural do direito para que ele se mantenha aderente à realidade socioeconômica de cada época. Nós vimos atualizando as Leis no tocante à Internet. Foram alterados o Código Penal (crimes digitais contra a Administração Pública), o Código de Processo Civil (uso de assinatura com certificado digital), o Estatuto da Criança e do Adolescente (crime de pedofilia), foram criadas leis para cibercafés e *lanhouses* (veja item 7.5, p. 85-86). O Brasil, em alguns aspectos, tem leis mais rígidas (ex.: nossa Constituição Federal proíbe o anonimato no art. 5º, IV, ao mesmo tempo que garante a liberdade de expressão, então não há direito de ser anônimo na Internet no Brasil), mas é mais carente (deficiente) no sentido de capacitar investigação pelas autoridades (ferramentas técnicas, treinamento, agilidade pois, se deve agir rápido para não se perder as provas eletrônicas).

Entendo que há três razões para o aumento de crimes digitais: 1º) Crescimento dos usuários de Internet e demais meios eletrônicos (celular, atm etc.) principalmente junto à baixa renda (classes C e D) e que se tornam vítimas fáceis, pois ainda não possuem cultura de uso mais seguro. 2º) Quanto mais pessoas no meio digital, os bandidos profissionais (quadrilhas) também migram, e então há maior ocorrência de incidentes. 3º) Falta de conscientização em segurança da informação, a maior parte das pessoas acha que nunca vai ocorrer com ela, empresta a senha, deixa o computador aberto e ligado, não se preocupa em usar as ferramentas de modo mais diligente, isso somado com uma dose de inocência potencializa as ocorrências.

Um incidente eletrônico gera maior dano, pois ocorre em geral de forma covarde, sem chance de defesa, além de gerar consequências que se perpetuam, pois a Internet é global e é difícil limpar totalmente uma informação dela. Por mais que haja retratação, uma publicação roda o mundo em poucos minutos.

Ou seja, merece punição exemplar, e tem sido comum o juiz determinar aumento de pena quando ocorreu no meio digital.

Devemos acompanhar atentamente todos os projetos de lei para Internet²⁶⁶. Inclusive o de crimes eletrônicos, agora a discussão de uma lei civil mais voltada para privacidade de dados. Precisamos quebrar paradigmas. Legislar sobre estes novos temas não é fácil. Há ainda desafios conceituais, como o crime de furto (art. 155), em que configura o tipo penal tornar indisponível coisa alheia móvel. Logo, na era dos dados, copiar e colar não tipifica furto? Só se der “ctrl X”. Devemos reescrever isso, mas sem também tipificar como furto toda situação. Não há lei perfeita, mas lei necessária. Temos de pegar a quadrilha que envia *e-mail* falso e não o inocente que passa para frente um *e-mail* falso sem saber que está mandando vírus para outra pessoa. Vivemos um momento desafiador, instigante e é uma oportunidade para pensarmos, criarmos as bases legais das próximas gerações. Temos de inovar, isso significa que nem tudo vai ser resolvido no Judiciário, há tendência para autorregu-

266. Lista dos projetos de lei que impactam a vida dos usuários de Internet e merecem ser acompanhados:

PL n. 5.470/2009 — Obriga as pessoas jurídicas de direito privado a fazer constar, de suas páginas da Internet, sua razão social, seu número no registro junto ao Cadastro Nacional de Pessoas Jurídicas — CNPJ e endereço da sede e sucursais e dá outras providências.

PL n. 5.361/2009 — Combate a pirataria — quer obrigar os provedores de acesso à Internet, em funcionamento em território nacional a identificar os usuários de seus serviços que estejam baixando, procedendo *download*, compartilhando ou oferecendo em sítios de qualquer natureza obras protegidas por direito autoral sem a autorização dos autores das obras.

PL n. 5.398/2009 — Dispõe sobre a identificação dos usuários dos serviços de correio eletrônico. O projeto foi arquivado.

PL n. 5.298/2009 — Estabelece a obrigatoriedade de cadastramento e de identificação eletrônica para fins de acesso à rede mundial de computadores, e de manutenção dos dados informáticos pelo período de dois anos para fins de investigação criminal ou instrução de processo penal. O projeto foi arquivado.

PL n. 4.996/2009 — Dispõe sobre a criação de cadastro nacional de consumidor para proibição do recebimento de propagandas por meio de telemarketing, mensagens eletrônicas e meios análogos. O projeto foi arquivado.

PL n. 4.805/2009 — “Cidadão digital” — visa permitir subscrição de projetos de lei de iniciativa popular por meio de assinaturas eletrônicas.

PLC n. 170/2008 — Quer alterar o art. 375 do CPC para que fique mencionado claramente que *e-mail* é prova documental.

PL n. 2.186/2003, 1.227/2007 e 4.187/2008 — Trata da questão do *spam* para coibir o envio de mensagem não solicitada por meio de redes de computadores destinadas ao uso do público. Todos estes projetos foram arquivados.

PL n. 1.429/2011 — Trata da restrição ao monitoramento de correspondência eletrônica por parte do empregador.

lamentação, para uso de arbitragem. Mas o maior esforço envolve a proteção das fronteiras de informação, a discussão do novo modelo de soberania dos Estados em um mundo cada vez mais plano. Como proteger os ativos, os recursos, e isso chega até a discussão de ciberguerra, biotecnologia, nanotecnologia, bioética e ciberética. Como não dá para puxar da tomada, temos sim muito trabalho a fazer.

8.36. A fraude eletrônica e os perfis falsos

O tema fraude eletrônica está inserido dentro do estudo de crimes eletrônicos. O motivo pelo qual ele é tratado em capítulo próprio é devido à necessidade de detalhamento maior, já que esta prática tem crescido muito, especialmente no tocante à modalidade de furto mediante fraude (art. 155 do Código Penal) no qual há envio de um *e-mail* falso (*phishing*) para um usuário e são capturados dados de sua conta bancária mediante a instalação de um arquivo malicioso em seu equipamento.

Toda fraude, independentemente da sua natureza, tem como pressuposto a utilização de um subterfúgio para ludibriar a vítima, seja por meio da ação ou da omissão do agente, isto é, o fraudador fornece informação errônea à vítima ou ainda omite.

Segundo Antônio de Loureiro Gil, em sua obra *Fraudes informatizadas*, estas correspondem a uma “ação intencional e prejudicial a um ativo intangível causada por procedimentos e informações (*software* e bancos de dados), de propriedade de pessoa física, ou jurídica, com o objetivo de alcançar benefício, ou satisfação psicológica, financeira e material”²⁶⁷.

As fraudes possuem duas origens: a) interna — quando praticadas por empregado ou terceiro que se encontram dentro do local a ser fraudado; e b) externa — o fraudador não possui vínculo com o local que será fraudado, mas isso não significa que o agente da fraude não possa um dia ter tido relação com a vítima.

Em termos de panorama da situação das fraudes eletrônicas em nosso país, o Brasil é tido como o maior exportador de crimes eletrônicos do mundo e, obviamente, as fraudes estão inclusas nessas estatísticas.

267. GIL, Antônio Loureiro. *Fraudes informatizadas*. 2 ed. São Paulo: Atlas, 1999. p. 15.

Cabe ainda destacar que, para combater o crime eletrônico, foi realizada a Convenção de Budapeste²⁶⁸, sobre cibercriminalidade do Conselho da Europa, documento de Direito Internacional Público, elaborado por um comitê de peritos, que se pretende venha a ser adotado por todos os países.

Desse modo, segundo o CERT-BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), a fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros²⁶⁹.

Normalmente a fraude por “Phishing Scan” ocorre da seguinte forma: (1) um código malicioso é enviado por e-mail para as vítimas; (2) as quais, não analisando a veracidade do conteúdo nem o remetente da mensagem, acessam a informação, executam o arquivo e, conseqüentemente; (3) o computador do usuário é infectado; (4) comprometendo suas informações confidenciais, tais como senhas, dados pessoais etc.; (5) essas informações são transmitidas para o fraudador; (6) que as utiliza para acessar, por exemplo e (7) o Internet Banking da vítima e desviar dinheiro para outra conta²⁷⁰.

Conforme já foi exposto anteriormente, o delito virtual é, em princípio, um crime de meio, ou seja, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, caracterizando, assim, uma modalidade que só ocorre no ambiente virtual, à exceção de alguns tipos cometidos por hackers, que, de algum modo, podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, sendo, dessa forma, aplicável o Código Penal brasileiro. Nota-se que, em certos casos, o meio de materialização da conduta criminosa pode ser virtual; contudo, o crime não, como, por exemplo, ocorre na modificação ou alteração não autorizada de sistemas de informações, previsto no art. 313-B do CP.

268. Ver Convenção de Budapeste — <<http://conventions.coe.int/Treaty/cn/Treaties/Html/185.htm>>.

269. Conforme Cartilha em <<http://cartilha.cert.br/glossario/>>.

270. Para saber mais dados sobre fraude eletrônica, acessar <<http://www.cartilha.cert.br/>>.

Há quem entenda que no caso do *Phishing Scan*, aplica-se o art. 171 do Código Penal (e não o art. 155 de furto mediante fraude), isto é, crime de estelionato, que é descrito como “obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”.

No Brasil, a tendência é de que sejam tipificadas algumas condutas criminosas próprias da Internet. O Senador Eduardo Azeredo propôs um projeto de lei, na forma de um Substitutivo (PLS — Projeto de Lei Substitutivo), que reúne outros 3 três projetos: 76/2000, 137/2000 e 89/2003, e tipifica novas condutas criminosas envolvendo a informática, entre elas a obtenção de informações pessoais e segredos de negócios, além de determinar que sejam considerados crimes o acesso indevido a redes de computadores e a veiculação de pedofilia pela rede. O projeto também altera o Código Penal Militar e de Processo Penal Militar.

Um exemplo de crime atual que gera polêmica é o de furto de dados. Dado que o art. 155 do Código Penal define furto como “subtrair, para si ou para outrem, coisa alheia móvel”, a questão que se coloca e tem que ver com interpretação da doutrina, é se seria possível tipificar como furto a conduta de levar dados da empresa, mas deixá-los também, ou seja, sem eliminá-los ou apagá-los. Desse modo, não haveria indisponibilidade do bem, o que se entende como requisito de subtração.

Logo, esses ajustes na lei penal ajudariam a evitar situações de ter de optar por outro enquadramento, e, em vez de furto, cuja pena é de reclusão de um a quatro anos, e multa, ter-se-ia o crime de dano, cuja pena é bem menor, prevista no art. 163, de detenção de um a seis meses. Isso também impacta a questão do uso de monitoramento, na hipótese de pedido de interceptação por ordem judicial.

Esse número absurdamente alto de fraudes eletrônicas decorre de duas grandes problemáticas: a falta de conhecimento do usuário, que provém justamente da pequena veiculação de informações sobre o tema; e a falta de recursos humanos e tecnológicos das autoridades policiais.

Diante do cenário caótico apresentado, a melhor maneira de evitar as fraudes eletrônicas ainda é por meio da conscientização dos usuários, e para tanto seguem algumas recomendações:

- 1) não abrir arquivos anexados, pois geralmente são programas executáveis que podem causar danos ao computador ou capturar informações confidenciais;
- 2) não clicar em links para endereços da Internet, mesmo que conste o nome da empresa ou instituição, ou, ainda, mensagens como “clique aqui”;

3) em caso de dúvidas sobre a origem e veracidade de determinada mensagem, procurar excluir o *e-mail* evitando executar seus anexos ou acessar os *links* presentes em seu conteúdo;

4) em casos de contaminação por vírus ou outro código malicioso, reformatar a máquina, reinstalar totalmente o sistema operacional e os aplicativos, evitando restaurar *backups* antigos;

5) utilizar *softwares* de proteção (antivírus, anti-*spam*, anti-*spyware* e *firewall* pessoal) nos computadores de uso doméstico e corporativo, mantendo-os com as versões, assinaturas e configurações atualizadas;

6) não emprestar sua senha de *e-mail*, de Internet, de rede da empresa em hipótese alguma;

7) duvidar do perfil de pessoas que se comunicam em ambientes não seguros e anônimos, como Orkut, *Messenger*, *blogs*, *chats*, evitando clicar e abrir imagens, principalmente;

8) denunciar na delegacia de crimes eletrônicos, bem como também em *sites* especializados, como o “www.denunciar.org.br”.

É preciso, portanto, ter total cautela ao verificar o conteúdo de uma mensagem eletrônica, além de procurar meios seguros e eficientes de proteção contra os riscos presentes na utilização dos benefícios trazidos pela Internet.

Mister se faz distinguirmos o criminoso digital profissional, que em geral tem operado em quadrilhas, daquele que é oportunista. Ou seja, uma brecha de segurança, uma situação de momento, uma motivação de fama, dinheiro rápido ou mesmo vingança é que o provoca a passar dos limites da ética e da legalidade e se arriscar em uma aventura digital que pode lhe trazer prejuízos bem reais.

Definitivamente, a medida mais efetiva de combate ao crime digital tem a ver com aumentar a capacidade de prova de autoria (ex.: identidade digital obrigatória) bem como a definição de uma regra clara para guarda dos dados e *logs* de acesso à Internet ou à caixa postal de *e-mail* para toda empresa que prouver este tipo de serviço, pago ou gratuito. Já há leis em vigor relacionadas ao uso de cibercafé e *lanhouse*, no entanto, as mesmas deveriam alcançar inclusive *campus* universitário já que muitos dos incidentes têm envolvido acessos feitos nessas localidades, bem como em telecentros (loais de inclusão digital), hotéis e mesmo redes corporativas de empresas que permitem uso particular ou carecem de controle de autenticação (fomentando a prática do anonimato).

Se a Constituição Federal de 1988 veda o anonimato em seu art. 5º, IV, justamente pois isso favorece e estimula a prática delituosa, a não ser em caso

de exceção (ex.: denúncia anônima), como uma prefeitura coloca acesso *wi-fi* sem qualquer controle de identidade de usuários? No caso, por envolver administração pública, será aplicável o princípio de responsabilidade objetiva, mesmo sem culpa, bem como o ônus de ressarcir os danos causados a vítima.

Nesse sentido, é extremamente grave a situação de criação de perfis falsos e mesmo a prática de falsa identidade digital, conhecida como incidente de *identity thief*, que contribui muito para aumentar a insegurança na *web*. Mas como combater esse tipo de crime?

A primeira estratégia de prevenção envolve o registro prévio da identidade. Ou seja, para evitar que alguém se passe facilmente por outra pessoa ou pela marca, o ideal é criar rapidamente o seu perfil nas principais redes sociais. Em seguida, com isso, deve-se divulgar que aquele é o perfil oficial. Parece simples, mas muitas empresas ainda negligenciam essa atitude preventiva. Acabam fazendo o registro só depois que já foram vítimas de um perfil falso.

No âmbito corporativo, é importante destacar que faz parte da estratégia de prevenção não apenas o registro do perfil oficial, mas principalmente o registro da Marca no INPI. Apesar de ser uma recomendação básica e simples, ainda há muitas empresas que somente se preocupam com o registro do domínio para disponibilizarem seu *site* na Internet, mas esquecem de formalizar a proteção de sua marca no Brasil e em outros países. A empresa que possui marca registrada pode-se valer da proteção legal conferida pela Lei n. 9.279/96, art. 130, III, e art. 189, I, em caso de incidentes.

Mesmo não tendo a marca registrada, a empresa pode ainda pleitear a proteção com base no art. 1.166 do Código Civil Brasileiro: “a inscrição do empresário, ou dos atos constitutivos das pessoas jurídicas, ou as respectivas averbações, no registro próprio, asseguram o uso exclusivo do nome nos limites do respectivo Estado”. Vale, porém, lembrar que o registro confere mais força e legitimidade ao ofendido caso a ocorrência tenha de ser levada até o Judiciário.

Além disso, a proteção ao nome empresarial decorre do direito fundamental garantido pela Constituição Federal, no art. 5º, XXIX: “todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) XXIX — a lei assegurará aos autores de inventos industriais privilégio temporário para sua utilização, bem como proteção às criações industriais, à propriedade das marcas, aos nomes de empresas e a outros signos distintivos, tendo em vista o interesse social e o desenvolvimento tecnológico e econômico do País”.

A segunda estratégia é a monitoração. Qualquer pessoa hoje deve ficar vigilante com o que aparece sobre si mesmo e que possa afetar sua reputação digital. Deve fazer buscas periódicas para ver se encontra algo que possa ser ilegítimo, equivocado ou mesmo ilícito. Esse exercício contínuo de monitorar o que aparece associado ao seu nome ou à sua marca, incluindo buscas por imagens e pesquisas dentro das redes sociais, ajuda a evitar riscos e possibilita a adoção de rápidas providências em caso de haver algum tipo de incidente, minimizando os danos e prejuízos.

A terceira estratégia é a do diálogo e transparência. Se a pessoa ou marca identificar que há um perfil criado em seu nome, por outra pessoa, deve fazer uma primeira abordagem amigável no perfil para entender a intenção do titular e comunicar que o perfil oficial está criado, propondo a migração daquela comunidade para o perfil oficial. Nesse ponto, no tocante às empresas, devem-se diferenciar alguns tipos de casos que merecem atenção específica: a) perfil criado por consumidor; b) perfil criado por colaborador; c) perfil criado por fornecedor ou parceiro; e d) perfil criado por terceiro (qualquer outra pessoa sem vínculo algum com a empresa).

Dependendo de quem criou o perfil e do contexto do conteúdo associado, pode ser necessário realizar uma abordagem mais voltada ao atendimento ao cliente e comunicação (SAC), ou mais direcionada ao relacionamento com equipes (RH), ou ainda optar pelo envio de notificação extrajudicial ou pela adoção de medidas judiciais (jurídico), conforme a gravidade do incidente. Nesse último caso, recomenda-se o registro de Ata Notarial, junto a um Cartório de Notas, para preservação da prova.

Conforme a resposta, ou na ausência dela, passa-se a tratar a permanência do perfil falso como um incidente que deve ser reportado ao provedor do serviço de rede social. Cada um deles possui um canal próprio de denúncia, que deve ser a primeira alternativa, caso não haja solução amigável entre as partes. Ali, a partir da denúncia, normalmente o perfil que infringe os termos de uso é removido rapidamente.

Os Termos de Uso do Facebook, por exemplo, dizem o seguinte: "(...) *Proteção dos direitos de outras pessoas: Nós respeitamos os direitos de outras pessoas, e esperamos que você faça o mesmo. Você não deve publicar conteúdo ou tomar qualquer atitude no Facebook que infrinja ou viole os direitos alheios ou a lei. Nós podemos remover qualquer conteúdo ou informações publicadas por você no Facebook se julgarmos que isso viola esta declaração ou nossas políticas. Se você violar repetidamente os direitos de propriedade intelectual de outras pessoas, desativaremos sua conta quando julgarmos apropriado. Você não deve marcar usuários nem enviar convites*

por e-mail para não usuários sem o consentimento deles. O Facebook oferece ferramentas de denúncia social para permitir que os usuários comentem sobre a marcação. (...)".

No entanto, caso a remoção não ocorra, cabe então o envio de notificação extrajudicial e ajuizamento de ação de obrigação de fazer com pedido de tutela antecipada liminar, para que o Juiz determine a retirada do perfil do ar, sob pena de multa diária em caso de descumprimento e até mesmo sob pena de apuração do crime de desobediência, caso o provedor se mantenha inerte. Essa ação ainda pode ser cumulada com pedido de ressarcimento pelos danos eventualmente causados pela não remoção do ilícito desde a ciência formal do provedor do serviço (realizada pela denúncia em seu canal oficial e envio da notificação).

Aliás, a inércia dos provedores quanto à adoção de medidas imediatas e que minimizem a exposição (e, conseqüentemente, os danos) das vítimas no meio virtual já tem sido tema de diversas decisões pelo Judiciário, de modo que, recentemente, o Superior Tribunal de Justiça (STJ) muito bem decidiu sobre o tema:

"Responsabilidade civil. Internet. Redes sociais. Mensagem ofensiva. Ciência pelo provedor. Remoção. Prazo. A velocidade com que as informações circulam no meio virtual torna indispensável que medidas tendentes a coibir a divulgação de conteúdos depreciativos e aviltantes sejam adotadas célere e enfaticamente, de sorte a potencialmente reduzir a disseminação do insulto, minimizando os nefastos efeitos inerentes a dados dessa natureza. Uma vez notificado de que determinado texto ou imagem possui conteúdo ilícito, o provedor deve retirar o material do ar no prazo de 24 (vinte e quatro) horas, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. Nesse prazo de 24 horas, não está o provedor obrigado a analisar o teor da denúncia recebida, devendo apenas promover a suspensão preventiva das respectivas páginas, até que tenha tempo hábil para apreciar a veracidade das alegações, de modo a que, confirmando-as, exclua definitivamente o perfil ou, tendo-as por infundadas, restabeleça o seu livre acesso. O diferimento da análise do teor das denúncias não significa que o provedor poderá postergá-la por tempo indeterminado, deixando sem satisfação o usuário cujo perfil venha a ser provisoriamente suspenso. Cabe ao provedor, o mais breve possível, dar uma solução final para o conflito, confirmando a remoção definitiva da página de conteúdo ofensivo ou, ausente indício de ilegalidade, recolocando-a no ar, adotando, nessa última hipótese, as providências legais cabíveis contra os que abusarem da prerrogativa de denunciar." Recurso especial a que se nega provimento" (STJ, REsp 1.323.754/RJ (2012/0005748-4), Rel. Min. Nancy Andrighi, DJ 19-6-2012).

Convém acrescentar, ainda, que a identificação da autoria do responsável pela criação do perfil também é possível, caso seja do interesse do ofendido, com grandes chances de êxito.

Os canais oficiais para denunciar incidentes são:

- *Youtube* — Para denunciar um vídeo impróprio ou que atente contra o direito de alguém, deve-se clicar no botão “Sinalizar” abaixo do vídeo ou, nos demais casos, acessar: <http://support.google.com/youtube/bin/request.py?hl=pt-BR&contact_type=abuse&crd=1>.

- *Twitter*: <<https://support.twitter.com/groups/33-report-abuse-or-policy-violations>>.

- *Facebook*: <<https://www.facebook.com/report/>>.

Na Califórnia, já há lei específica para penalizar quem cria perfil falso ou usa identidade falsa na *web*. Essa conduta tem sido tratada como “grave” em muitos países, pois gera quebra de confiança na rede e aumenta a insegurança digital, partindo do pressuposto de que, quando as relações são não presenciais, é fundamental acreditar que a pessoa do outro lado da interface gráfica é quem ela diz ser.

Por isso, deve-se ter uma estratégia de proteção de Nome, Marca e Reputação Digital bem implementada, que envolva uma atuação conjunta das áreas de Comunicação, Jurídico, SAC e RH. Afinal, a exposição digital indevida gera danos bem reais!

Essas medidas exigem amparo legislativo para que tenham eficácia e sejam mandatórias para todos, a que custo for. Se para passar por fronteiras físicas é requisito a identificação legal com documento válido, por que não para atravessar fronteiras virtuais?

Em seguida, deve-se investir na educação dos usuários e dos operadores do direito. No primeiro caso, para que eles saibam se proteger (o que aumenta a prevenção dificultando a vida dos bandidos), bem como saibam reagir em uma situação de incidente no sentido de saber preservar as evidências (provas eletrônicas), saber dar andamento em uma denúncia (ex.: a vítima leva ou não seu computador até a delegacia, pode fazer B.O. em qualquer uma ou só na especializada) e até mesmo exercer, quando aplicável e excepcionalmente, a legítima defesa digital (arts. 23 e 25 do Código Penal) para sua própria salvaguarda, visto as exigências de respostas imediatas em situação de perigos iminentes e em tempo real da Internet. No segundo caso, investindo em treinamento e ferramentas tecnológicas que permitam de fato realizar as investigações necessárias na solução dos crimes digitais e na punição dos culpados.

Somente com campanhas maciças da população em geral, com treinamento, com adoção de aulas de “cidadania e ética digital” como disciplina obrigatória na grade de ensino médio e fundamental de escolas públicas e particulares, poderemos criar um “usuário mais protegido e também mais ético”, combatendo consideravelmente o crime eletrônico em sua raiz, visto que em muitos casos há certo desconhecimento, desatenção e negligência do usuário como agente facilitador da conduta, ou há uma despreocupação com as leis, uma “falta de noção” das consequências, estimulando o criminoso eletrônico oportunista.

Por último, deve-se redigir os novos artigos relacionados a tipificação dos crimes digitais, bem como o aumento de pena daqueles em que o ambiente computacional é apenas meio de execução do crime (ex.: crimes contra a honra), mas em conjunto com uma alteração (atualização) da Lei de Execuções Penais, para que seja repensado o modelo de cumprimento da pena e de reintegração deste tipo de criminoso na sociedade. Não podemos correr o risco de deixar preso na mesma cela o criminoso tradicional, analógico (versão 1.0) com o criminoso digital (versão 2.0) e de lá sair o criminoso ainda mais evoluído e sofisticado (versão 3.0).

Por certo, um crime em ambiente digital é muito mais maléfico, tem um poder de alcance e devastação maior, sua conduta é possível de ser replicada com intermédio de máquinas (*softwares* e/ou robôs), ocorre em geral sem chance de defesa e de forma covarde. Por isso, se ocorrido em ambiente de Internet deveria sempre caracterizar a aplicação do aumento de pena, de forma a gerar punição exemplar e evitar a solução com o pagamento de apenas uma cesta básica.

Devemos rever a forma como tratamos o direito penal e processo penal na era digital sob pena de que sua obsolescência estimule que os usuários passem a preferir “fazer justiça com o próprio *mouse*” a se socorrerem das autoridades e do Judiciário.

8.37. A legítima defesa na Internet

Dentro da nova realidade da sociedade digital, é fundamental repensar alguns princípios jurídicos, bem como resgatar os valores aos quais tais princípios estão atrelados e que motivaram a existência das leis que se encontram em vigor. É preciso interpretar as normas legais de acordo com as novas situações, que merecem novas respostas.

Com a Internet, passaram a ser comuns situações de ataques, agressões, vandalismo e até mesmo crimes que ocorrem com pessoas físicas e jurídicas em

ambientes totalmente eletrônicos, não presenciais, em que as únicas testemunhas são as máquinas. É inteiramente normal que em qualquer desses casos, em que há uma situação de infração ou conflito de direito em âmbito real ou virtual, a vítima queira proteger-se.

Sendo assim, como fica a questão do exercício do direito de legítima defesa na Internet? Até onde a defesa pode virar infração? Até onde podemos atacar quem nos está atacando, mesmo para conseguir saber qual sua identidade e, então, entrar com uma medida judicial?

Por necessidade de aumentar a segurança da informação, muitas empresas no Brasil já possuem profissionais especializados em combater delitos virtuais, especialmente os cometidos por *hackers*. Em muitos casos, é formado um time de “resposta a incidente”, ou há um time de monitoramento para que se possa pegar o infrator literalmente com a “mão na máquina”, quer ele seja de dentro, algum funcionário ou colaborador, quer seja de fora (um próprio cliente que pode estar cometendo autofraude, parceiro, fornecedor ou terceiro).

Para isso, toma-se uma série de medidas, são compradas tecnologias específicas e muitas vezes também são contratadas empresas que praticam o que se chama “*Ethical Hacking*”. Mas, para o direito brasileiro, apesar da boa-fé de quem está trabalhando nessa área, pode ocorrer que a pessoa venha a ser considerada criminosa no exercício dessas atividades. A imputação mais comum é a de crime de falsa identidade (CP, art. 307), podendo chegar a possível “flagrante preparado”, crime de dano (CP, art. 163), crime de interceptação (Lei n. 9.262/96), entre outros.

Quando há um incidente, busca-se principalmente atender aos seguintes objetivos: 1) bloquear ou minimizar o ataque ou a vulnerabilidade; 2) descobrir quem é o causador, ou seja, a identidade do infrator; 3) coletar provas que possam ser utilizadas para responsabilização dele; 4) tomar as medidas para normalizar a situação, para que volte a ser como era no momento anterior ao incidente.

Mas se, para alcançar esses objetivos, não são aplicadas as boas práticas de Direito Digital e computação forense, o que pode ocorrer é que as provas coletadas sejam consideradas obtidas por meio ilícito (CC art. 213; CPC, art. 332; CPP, art. 386 etc.); bem como a empresa pode ser responsabilizada civilmente, e o profissional, criminalmente.

No entanto, se for situação de legítima defesa, isso não ocorre. É o que está previsto no art. 23, II, do Código Penal, que assim reza: “*Não há crime quando o agente pratica o fato: I — em estado de necessidade; II — em legítima defesa; III — em estrito cumprimento de dever legal ou no exercício regular de direito*”.

Para exemplificar, um analista muitas vezes consegue descobrir a conta de *e-mail* (ou de *ftp*) utilizada pelo fraudador para armazenar os dados obtidos ilegalmente, bem como a senha que dá acesso a essa conta. Entretanto, em termos jurídicos, a empresa poderia tentar obter de volta os dados que foram pegos pelo fraudador e minimizar os danos? A empresa poderia acessar a conta de *e-mail* deste terceiro, sem infringir a lei? Como validar as provas obtidas dessa maneira?

A prerrogativa da autodefesa é uma causa de justificação que se baseia no princípio de que o Direito não precisa retroceder diante do injusto e, ainda, de que a defesa vale, pois, não só para o bem jurídico ameaçado, mas também, simultaneamente, para a afirmação da ordem jurídica. Sendo assim, o art. 25 do Código Penal define: “*Entende-se em legítima defesa quem, usando moderadamente dos meios necessários, repele injusta agressão, atual e iminente, a direito seu ou de outrem*”.

Assim, verificamos que a defesa da vítima ou a ação de outro que venha a responder ao ataque não será passível de punição se sua atitude se enquadrar em legítima defesa. Para a Internet deve-se definir claramente o que significa o “emprego moderado dos meios necessários”. Nesse sentido, aplica-se o brocardo jurídico: *Nemo expectare tenetur donec percutietur* (ninguém — para defender-se — está obrigado a esperar até que seja atingido por um golpe).

Isso porque nem todo ato de defesa ou de autodefesa é legítimo, ou seja, autorizado pela ordem jurídica. O Direito impõe restrições relativamente precisas para que o indivíduo, por seus próprios meios, possa fazer prevalecer seus interesses ou bens diante do agressor, sem o concurso dos órgãos do Estado. Do contrário, é necessário estar munido de ordem judicial, ou então do poder de polícia, o que muitas vezes não ocorre no dia a dia das empresas.

A defesa está limitada ao uso restrito dos meios reputados eficazes e suficientes para repelir a agressão. Nem menos, nem mais do que isso. Ou seja, há um princípio de proporcionalidade que exige certa moderação. Nesse sentido, o parágrafo único do art. 23 dispõe que o excesso no exercício da legítima defesa implicará a responsabilização, por dolo ou culpa²⁷¹. Logo, é fundamen-

271. “O agente, em qualquer das hipóteses deste artigo, responderá pelo excesso doloso ou culposo”. Abaixo algumas jurisprudências relacionadas ao tema:

“Ação de indenização por danos materiais e morais. Autora que fundamenta a pretensão em operações realizadas indevidamente em sua conta corrente. Instituição financeira que não produziu provas aptas a demonstrar que as movimentações foram efetuadas pela correntista. Inteligência dos artigos 6º, inciso V, e 14, parágrafo 3º, do Código de Defesa do Consumidor.

tal que se verifiquem caso a caso, ou em um padrão de cenário específico, quais as medidas mínimas de defesa e em que momento as ações passam a configurar infrações.

Haverá casos em que o mero acesso à caixa postal usada pelo *trojan* para armazenar os dados dos clientes será medida suficiente. Por outro lado, poderá encontrar-se armazenada grande quantidade de informações que não podem permanecer em poder do *hacker* e deverão ser apagadas dos seus sistemas. O cancelamento das contas de *e-mail* também pode ser considerado uma medida eficaz e necessária, dentro do direito de legítima defesa, mas não se podem generalizar as condutas. Se alguém lhe enviar um *spam*, você não pode responder com um vírus!

Concluindo, é fundamental o treinamento das equipes, a elaboração de termos e códigos de conduta, bem como que os contratos com empresas que praticam “*Ethical Hacking*” já prevejam situações de limites de ações e de responsabilidades, para que se evite gerar riscos e contingências legais, quando se imaginava que se estava protegendo. Defender-se é uma coisa, atacar é outra!

Ato que acarreta a presunção dos prejuízos sofridos pela autora. Dever de indenizar é de rigor. Dano moral caracterizado. Manutenção da decisão. Negado provimento ao recurso” (TJSP, Apelação 0123424-98.2008.8.26.0002, rel. Des. Ligia Araújo Bisogni, j. 23-11-2011).

“Responsabilidade civil. Indenização. Danos morais. Empréstimo contraído por terceiros, por meio eletrônico, com débito das parcelas em conta corrente da autora. Negativação indevida da requerente. Responsabilidade objetiva do banco requerido pelos serviços prestados. Verba indenizatória devida. *Quantum* indenizatório bem mensurado. Recursos desprovidos. Sentença mantida” (TJSP, Apelação 0000676-15.2010.8.26.0125, rel. Des. Ademir Benedito, j. 26-10-2011).

“Administradora de cartão e sistemas de pagamento. Fraude. Recurso. Apelação. Alegação de que a ré tinha o ônus da prova da recusa de pagamento dos titulares de cartão de crédito pelo não reconhecimento da validade da compras devidamente autorizadas por ela não conhecida. Julgamento de recurso com alteração de pedido ou a causa de pedir deduzido na inicial afronta ao princípio do duplo grau de jurisdição e caracteriza julgamento *extra petita*, com violação do disposto nos arts. 128, 264, 460, 514, II, e 515, § 1º, do CPC. Cartão de crédito. Contrato de afiliação. Administradora do Sistema Visanet deve arcar com os valores relativos aos negócios jurídicos por ela autorizados, mesmo que não reconhecidos pelos titulares de cartão, na hipótese de cartões clonados, quando não demonstrado descumprimento pelo empresário vendedor de obrigações contratuais, visto que a responsabilidade pela segurança do sistema Visanet é da administradora que presta esse serviço, com incumbência de prover meios que impeçam a concessão de autorização para vendas realizadas com cartões de crédito clonados. Ausente prova do descumprimento pela autora fornecedora de obrigações contratuais relativamente às vendas devidamente autorizadas pela ré administradora, com base em cartões de crédito colados. Reforma para julgar procedente a ação. Recurso provido” (TJSP, Apelação 0154088-12.2008.8.26.0100, rel. Des. Rebello Pinho, j. 15-8-2011).

8.38. Publicidade online

A publicidade na Internet é um ensaio para um mundo de convergência entre a rede mundial de computadores e a *TV broadcasting*, que já existe com a TV Interativa em vários países. A publicidade virtual é bem diferente da tradicional veiculada na TV ou nas demais mídias. A particularidade da mídia virtual é que, tecnologicamente, é possível finalizar operações comerciais a partir de um simples anúncio. Assim, o objetivo da publicidade — e seu limite — não é apenas a sedução do comprador: uma vez e imediatamente após o momento em que for seduzido, pode ele adquirir o produto com simples toques no *mouse*. A publicidade *online*, portanto, permite chegar até o final da operação, que é a realização da venda efetiva, principalmente nas novas mídias convergentes como a TV Interativa.

Esse tênue limite entre o momento em que termina o anúncio e aquele em que começa a transação comercial tira o sono dos publicitários²⁷² e traz uma questão jurídica: de quem serão as responsabilidades no caso de propaganda enganosa?²⁷³ O publicitário não é mais aquele sujeito que opera num mundo em que todas as pessoas são absolutamente lindas e saudáveis e os produtos anunciados funcionam perfeitamente bem. Paradoxalmente, passa a ser quase que como o velho e tradicional vendedor de uma loja do mundo real, tendo de manter o convencimento do consumidor até o momento em que este desembolsa o dinheiro, assina o cheque, ou emite-se o comprovante do cartão de crédito/débito — no caso da Internet, até o momento em que o usuário dá o clique definitivo que finaliza a compra. No mundo real, o vendedor, ou a loja, juntamente com o fornecedor ou fabricante, são responsáveis por um produto que não cumpra as atribuições anunciadas; no mundo virtual, chega-se mais

272. Outra questão relevante que está causando grande receio entre os publicitários são as novas implicações trazidas pela nova indústria de comunicação. Nos contratos para mídias tradicionais como a TV, a responsabilidade se limitava à elaboração de um roteiro a partir do qual seria produzido o filme publicitário. Criavam apenas o roteiro e não a peça audiovisual. Nos contratos para as mídias digitais, o domínio da tecnologia é pré-requisito, os profissionais são responsáveis pela funcionabilidade da peça publicitária quando acessada; para se manterem no mercado, têm de se preocupar com aspectos técnicos e jurídicos, com os quais ainda não estão acostumados a lidar.

273. No Código de Defesa do Consumidor, a responsabilidade pela publicidade enganosa é, via de regra, do fornecedor do bem ou serviço (art. 30), já que estes anúncios são veiculados às expensas daquele (art. 10, § 2º). Quando, porém, a forma da propaganda permite que em um clique consumidor e fornecedor possam realizar uma operação de compra e venda, o veículo passa a realizar uma verdadeira relação de intermediação, adquirindo responsabilidades semelhantes às de um corretor, integrando, portanto, a cadeia de consumo.

uma vez à questão: onde termina a publicidade e onde começa a transação comercial? Quem é responsável pelo quê?

Tudo isso faz com que haja uma mudança não só do aspecto comportamental de mercado como dos próprios contratos de mídia, criando-se contratos de Mídia Responsável e Mídia de Resultado, já que, a mídia não apenas dá a veiculação do anúncio, medido no aspecto de audiência e retorno com a visibilidade da marca, mas vai ser medida no aspecto de participação e venda, visto que alcança o consumidor capacitado para efetuar uma compra real, mediante um clique. Essa nova mídia, em termos de tecnologia de banco de dados relacional, tem capacidade de gerar um banco de dados de consumo como nunca houve, o que nos leva à questão da privacidade das informações. Para isso é bom distinguir dados cadastrais de dados comportamentais e relacionais.

Os dados comportamentais são aqueles produzidos por *softwares* que acompanham o comportamento individual de consumo na Internet, associam ações e resultados como uma pesquisa *online*, sendo de propriedade das empresas que os prospectam, portanto, negociáveis²⁷⁴.

Existem vários meios de publicidade na Internet. Os *banners* são os mais comuns e também os mais problemáticos para quem anuncia. Sua eficiência é cada vez mais contestada, porque um clique num *banner* normalmente significa um desvio de rota, o que é pouco desejável pelo usuário. Começam a surgir mecanismos, como os *hotsites* e *websites* de destino, que permitem encaminhar o consumidor para o local desejado pelo usuário, sem desviá-lo de sua rota, mas induzindo-o a traçar uma rota desejada pelo anunciante. Isso faz com que a estratégia de comunicação alcance um resultado que pode ser mensurável, muito mais que no formato tradicional.

O caráter da publicidade virtual é de abordagem direta, durante o processo de comunicação. Essa tendência será acelerada pela convergência com a TV: não serão mais necessários intervalos comerciais (o que vamos chamar de comunicação de interrupção: o programa para momentaneamente para que anúncios sejam veiculados), mas os anúncios serão veiculados na tela durante a exibição do conteúdo, possibilitando o acesso imediato a outros ambientes virtuais (como ocorre nos *sites* hoje, com a proliferação de *links* comerciais no *display* do usuário).

274. Os dados pessoais dos consumidores são protegidos constitucionalmente pelo art. 5º, X, e os cadastros com esses dados elaborados são regulamentados pelo Código de Defesa do Consumidor nos arts. 43 e 44. No entanto, bases de dados coletados durante a navegação, pelos provedores, constituem propriedade intelectual, protegida pela Lei n. 9.610/98, art. 7º, XIII — Lei de Direitos Autorais —, garantindo ao seu autor os direitos morais e patrimoniais sobre as obras que criou, elencados no art. 87 da referida lei.

Aparentemente, esse é um mundo mais invasivo e traz riscos que não podem ser menosprezados. Em algumas situações, a publicidade virtual pode vir a, em seu conjunto, causar prejuízo ao receptor. O envio excessivo de publicidade no *e-mail* pode provocar a perda de mensagens da caixa postal do usuário — o que não ocorre nas televendas convencionais, quando somos maciçamente abordados por ligações de *call centers* para venda de algum produto ou para pesquisas de *marketing*. Por isso, a abordagem de interrupção deve ser substituída por um *marketing* de permissão. Não apenas como uma estratégia de comunicação, mas principalmente por uma consequente responsabilidade civil pelos danos eventualmente causados aos usuários receptores.

A tecnologia oferece ferramentas para proteger o usuário dos excessos da publicidade virtual. Ele pode optar por receber ou não anúncios publicitários sucessivos enquanto assiste a um programa — gerando o que podemos chamar de uma comunicação de permissão. A liberdade de escolher se quer ou não ter acesso à publicidade será, mais do que nunca, do consumidor. Essa questão tem que ver com a privacidade. Como cada indivíduo tem uma visão diferente do que seria invasão de privacidade, é desejável que a legislação brasileira esteja preparada para exigir que os operadores do mundo da convergência cumpram determinadas obrigações e limites para não lesar o direito de seus consumidores.

Acontece que os publicitários e demais empresários da comunicação não estão acostumados ao livre arbítrio do consumidor (atualmente um ser passivo, obrigado a assistir ao intervalo comercial — com, no máximo, a possibilidade de mudar para um canal onde não esteja ocorrendo tal intervalo). O consumidor digital passa a ser ativo, decidindo se quer ou não ver qualquer comercial e quando quer assisti-lo.

A lei não deve criar restrições sobre o que poderá ser veiculado, mas deve obrigar os veículos a informar e dotar o consumidor de capacidade para escolher o que ele quer ou não receber. Alguns princípios são básicos, portanto, para que a privacidade seja preservada: por exemplo, a utilização de banco de dados sem a autorização daqueles que estão cadastrados configura invasão de privacidade, mas a solicitação de conferência de dados para efetuar uma transação, não. Outro exemplo: malas diretas, publicidade virtual e outros itens só podem ser recebidos mediante autorização do usuário. É muito simples e pode ser entendido em relação a uma tecnologia amplamente utilizada hoje: o envio de publicidade por *e-mail*. A empresa pode enviar um *e-mail* para um usuário comunicando que este está em sua mala direta e pedindo permissão para enviar *e-mails* periódicos anunciando seus serviços. A omissão de resposta ou uma resposta negativa significariam, automaticamente, que o usuário não quer re-

ceber *e-mails* dessa empresa; poderia haver uma lei determinando que o rompimento desse trato é uma violação (esse raciocínio se aplica a malas diretas por *e-mail* e não às do mundo real, porque o primeiro caso configura uma despesa muito pequena para as empresas, o que incentivaria o abuso).

Resolver essa questão o quanto antes significa preservar a privacidade dos futuros consumidores digitais, sem gerar uma carga excessiva e detalhada de proibições legais. Como dissemos, é um raciocínio baseado em direitos e deveres, em permissão e obrigações, mas não em proibições *a priori*. A tecnologia está do lado dessa nova visão, para preservar o bem comum no momento em que a virtualidade chegar à comunicação em massa.

O uso de banco de dados e seus limites éticos sempre irá gerar muita discussão, mas aqui o principal aspecto refere-se à coibição do abuso da emissão de *e-mails* não solicitados pelos destinatários. Portanto, para o Direito Digital, deve haver a prática de uma publicidade responsável, com o compromisso de consultar o consumidor antes de simplesmente enviar as mensagens publicitárias. Isso é uma mudança comportamental, e cabe ao Direito contribuir para que ela ocorra mediante sanções pecuniárias, como as já determinadas pelo Código Civil e pelo Código de Defesa do Consumidor.

8.39. A questão do *spam* e do *e-mail* marketing²⁷⁵

O *e-mail* já se tornou uma das principais ferramentas de comunicação, competindo talvez mais com comunicadores instantâneos em alguns públicos ou segmentos, mas por certo, já é da rotina da grande maioria das pessoas. Em muitos casos, é o único veículo de contato e de estabelecimento de direitos e obrigações entre as partes, já havendo “*e-mail-vale oferta*”, “*e-mail-contrato*”, “*e-mail-de acordo*”, “*e-mail-notificação*”, “*e-mail-reclamação*”, entre outros.

Com isso, cresce a importância de saber usar esta ferramenta de forma ética e legal. Como uma empresa que faz comunicação por *e-mail* marketing deve proceder para evitar ser taxada como “*spammer*” e ao mesmo tempo também conseguir gerar maiores resultados de vendas e de fidelização?

Ao mesmo tempo que cresce o uso de *e-mail*, mensagens de texto, uso de comunicadores instantâneos, mensagens de celular, o *spam* vem se tornando um mal da era digital tendo em vista o direcionamento que ele vem tendo, porque, além de ser uma mensagem não solicitada, na maioria das vezes possui conteúdo falso, remetente falso, não tem a possibilidade de o destinatário so-

licitar que a mensagem não seja mais enviada e ainda é usado para a transmissão de vírus, códigos maliciosos (programas que executam ações maliciosas em seu computador, como, por exemplo, destruir arquivos, retirar informações etc.), *phishing scam* (mensagens enviadas a um grande número de usuários com a finalidade de induzir a pessoa a clicar em um *link*, que instalará códigos maliciosos na máquina, objetivando monitorar a navegação na Internet, furtar dados, tais como senha de banco, número de cartão de crédito, informações armazenadas no HD do computador etc., entre outros.

São vários os projetos de lei propostos sobre a matéria. Na Câmara dos Deputados destaca-se o PL n. 2.186/2003, que dispõe sobre o envio de mensagem não solicitada por meio de redes de computadores destinadas ao uso do público.

Ao PL n. 2.186/2003 estão apensados os PLS n. 2.423/2003, 3.731/2004, 3.872/2004, 1.227/2007 e 4.187/2008.

O PL n. 2.186/2003 obteve voto favorável na forma do substitutivo oferecido pelo Deputado Nelson Proença e desde dezembro de 2008 encontra-se na Comissão de Constituição e Justiça e de Cidadania para apreciação do Deputado Leonardo Picciani (PMDB-RJ).

Os PLS n. 2.186/2003 e 1.227/2007 permitem o “primeiro envio”, ou seja, a possibilidade de enviar uma única vez uma mensagem não solicitada, a fim de obter o consentimento do destinatário para continuar o envio.

Já o PL n. 4.187/2008 permite o envio de mensagens eletrônicas não solicitadas desde que a mensagem traga em seu corpo, entre outros requisitos, o procedimento para que o destinatário opte por não recebê-la mais, ou seja, enquanto o usuário não informar que não tem interesse em receber mensagens deste remetente o envio é permitido.

Permitir o primeiro envio é uma questão polêmica, pois há meios de alteração do remetente, por exemplo, mensagens com o mesmo conteúdo podem ser enviadas várias vezes por meio de *e-mails* rotativos, além de contribuir para o envio de *e-mails* fraudulentos.

O substitutivo do PL n. 2.186/2003 permite o envio de mensagens eletrônicas com conteúdo comercial desde que os destinatários tenham optado por recebê-las ou haja relação comercial preexistente entre o remetente e o destinatário. Porém, não prevê que o remetente deve obrigatoriamente inserir no corpo da mensagem mecanismo ou procedimento para o destinatário manifestar a sua vontade de não mais receber tais mensagens.

Cabe também comentar o art. 5º do substitutivo do PL n. 1.227/2007, que acrescenta ao art. 307 do Código Penal o seguinte parágrafo:

275. Contribuiu para este item a Dra. Alice Andrade Frerichs.

“Parágrafo único. Incorre na mesma pena quem utilizar o endereço eletrônico de terceiro para o envio de mensagem eletrônica, ou reproduzir, em qualquer campo do cabeçalho ou do corpo de mensagem eletrônica, o nome, endereço eletrônico, marca ou logomarca de terceiro com a intenção de atribuir-lhe a autoria”.

A meu ver, é desnecessário tal acréscimo, pois o art. 307 do Código Penal que trata sobre falsa identidade é suficiente, cabendo ao juiz analisar o caso concreto e aplicá-lo.

No Senado destacam-se o PL n. 367/2003, que coíbe a utilização de mensagens eletrônicas comerciais não solicitadas por meio de rede eletrônica, e os projetos de lei a ele apensados, quais sejam, PLS n. 21/2004, que disciplina o envio de mensagens eletrônicas comerciais, e o PLS n. 36/2004, que dispõe sobre mensagens não solicitadas no âmbito da rede mundial de computadores.

Os referidos projetos encontram-se na Comissão de Educação para apreciação. O Senador Eduardo Azeredo em seu parecer concluiu pela aprovação do PLS n. 21/2004, na forma do substitutivo aprovado no âmbito da Comissão de Constituição, Justiça e Cidadania, e pelo aproveitamento parcial do PLS n. 367/2003 e do PLS n. 36/2004.

De acordo com o substitutivo do PLS n. 21/2004:

“Art. 3º É proibido o envio de mensagens eletrônicas não solicitadas”.

Mensagem eletrônica não solicitada, segundo o inciso II do art. 2º do referido Projeto de Lei, é *“toda mensagem enviada para destinatário não consentiente, e que, independentemente de sua finalidade, seja enviada de forma massificada, com conteúdo uniforme ou praticamente uniforme”*.

Assim, para o envio do *e-mail* ser legal, entre outros aspectos que o Projeto de Lei n. 21/2004 determina que sejam observados²⁷⁶, é importante que o destinatário seja consentiente, isto é, que:

276. *“Art. 4º O remetente de mensagem eletrônica é obrigado a apresentar, de forma clara e compreensível, em cada mensagem que enviar, os seguintes elementos:*

I — endereço físico ou endereço eletrônico do remetente;

II — mecanismo eletrônico eficaz pelo qual o destinatário possa facilmente exercer o direito de não mais receber mensagens daquele remetente.

Parágrafo único. No caso de coleta de dados do destinatário, deverá ser exibida declaração, de forma proeminente e compreensível, antes e durante o momento de coleta de informações, explicando quais dados pessoais serão coletados, quem os coletará, a maneira como serão coletados e utilizados, explicitando o uso de arquivos de armazenamento ou de outros mecanismos de rastreamento”.

a) solicite ao remetente ou consinta, de forma expressa, que este lhe envie mensagens eletrônicas;

b) tendo mantido contato social ou relação comercial prévia com o remetente, não manifeste oposição ao recebimento de mensagens eletrônicas, desde que, no momento do contato social ou da relação comercial, e em todas as mensagens subsequentes, tivesse à disposição mecanismo eficaz, simples e gratuito, pelo qual pudesse exercer a opção pelo não recebimento de mensagens eletrônicas desse remetente (inciso III, do art. 2º do PL n. 21/2004).

Ante o exposto, para o envio de *e-mail* eletrônico no âmbito comercial o remetente precisará obter a autorização do destinatário, que será expressa ou até mesmo derivada da conduta omissiva deste, uma vez que ele não optou pelo não recebimento de mensagens eletrônicas oriundas deste remetente.

O Projeto de Lei n. 21/2004 também veda o envio de *e-mail* para endereços eletrônicos obtidos a partir da utilização de programas de computador geradores de endereços de correio eletrônico, ou a partir da coleta automática de endereços de correio eletrônico feita em páginas da Internet (art. 5º do PL n. 21/2004).

O envio de mensagens não solicitadas ou, ainda, se autorizadas pelo remetente, mas estiverem em desconformidade com os requisitos mínimos exigidos pelo art. 4º do PL n. 21/2004, acarretará na penalização do destinatário ao pagamento de uma multa que poderá variar entre R\$ 50,00 (cinquenta reais) e R\$ 1.000,00 (mil reais)²⁷⁷.

Inclusive, além de estar sujeita à multa, a empresa responde solidariamente pelos danos causados pelo prestador de serviços por ela contratado para a realização de propaganda, publicidade ou mala direta, se para a execução do serviço o prestador infringir os dispositivos legais do Projeto de Lei n. 21/2004²⁷⁸.

277. PL n. 21/2004: Art. 7º: *“Sem prejuízo das ações previstas no Título III da Lei n. 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), fica sujeito à multa do art. 57 da mesma Lei, calculada por ofendido:*

I — no valor mínimo de cinquenta e máximo de quinhentos reais, quem infringir o art. 3º desta Lei;

II — no valor mínimo de cinquenta e máximo de cem reais, quem deixar de atender qualquer das exigências do art. 4º, quando o ato não constituir infração ao art. 3º desta Lei;

III — no valor mínimo de quinhentos e máximo de mil reais, quem infringir o disposto no art. 6º desta Lei”.

278. Art. 7º, § 1º: *“Fica sujeita à multa do caput, bem como é solidariamente responsável pelos danos causados aos ofendidos, a entidade que contratar serviços de propaganda, publicidade ou mala direta, quando o prestador dos serviços praticar qualquer das condutas vedadas nesta Lei”.*

Cabe ressaltar que o Projeto de Lei n. 21/2004 ainda será examinado pela Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática e, sendo aprovado, seguirá para a Câmara Federal. Todavia, este é o projeto que está mais próximo de tornar-se um dispositivo legal específico, abordando em seu texto o uso do *spam*.

Contudo, enquanto não é sancionada uma lei específica, é oportuno ressaltar que já temos dispositivos legais aplicáveis aos danos provocados por *spam*, como, por exemplo, o art. 307 do CP, o art. 187 do CC (inserido entre o rol dos atos ilícitos), alguns artigos do Código de Defesa do Consumidor, tais como os arts. 36 e 37 (segundo os quais a comunicação deve ser clara, de fácil identificação, não podendo ser enganosa e nem abusiva), os arts. 43 e 72 (que tratam sobre banco de dados) etc.

Nossos tribunais pátrios, embora timidamente em sua maioria têm se manifestado em favor do internauta:

"EMENTA: AGRAVO DE INSTRUMENTO. AÇÃO CAUTELAR INOMINADA. RESTABELECIMENTO DA PRESTAÇÃO DE SERVIÇO. ENVIO DE SPAMS. NECESSIDADE DE DILAÇÃO PROBATÓRIA. A partir das alegações das partes, uma sustentando tratar-se de envio de spams, atividade reconhecidamente ilícita, outra, que se trata de envio de e-mails marketing, atividade lícita, revela-se imperiosa a dilação probatória, o que será realizado nos autos da ação principal, com o intuito de se apurar, de forma efetiva, qual argumentação deve prevalecer. Manutenção da decisão agravada. NEGARAM PROVIMENTO AO AGRAVO DE INSTRUMENTO. UNÂNIME." (TJRS, Agravo de Instrumento n. 70025172263, Décima Oitava Câmara Cível, Relator: Nelson José Gonzaga, j. 2-10-2008).

"EMENTA: OBRIGAÇÃO DE NÃO FAZER. ENVIO DE E-MAILS. SPAM. A sentença recorrida é clara e se atém aos limites do pedido, ou seja, que a parte demandada se abstenha de remeter ao autor os chamados spam que são mensagens eletrônicas não solicitadas, quase sempre com o cunho publicitário. SENTENÇA MANTIDA. RECURSO DESPROVIDO." (TJRS, Recurso Cível n. 71001280536, Terceira Turma Recursal Cível, Turmas Recursais, Relator: Carlos Eduardo Richinitti, j. 7-8-2007).

Se o internauta sentir-se ofendido moralmente em razão do envio dos *spams*, poderá pedir a reparação dos danos causados. Contudo, a admissibilidade deste pedido tem sido encarada com parcimônia por nossos tribunais:

"EMENTA: Indenizatória. Provedor de Internet. Ataque de spam. Origem das mensagens. Comprovação. Dano material. Configuração. Pessoa jurídica. Honra objetiva. Ofensa ausente. Dano moral. Não configuração. Comprovada a origem das mensagens que configuraram ataque de spam, que obrigou o provedor de internet a adotar medidas para recuperação do normal

funcionamento do acesso à rede mundial de computadores para seus clientes, são indenizáveis os danos materiais daí decorrentes. Inexiste direito à indenização por dano moral para a pessoa jurídica quando não comprovada ofensa à sua honra objetiva, caracterizada pela fama, conceito e credibilidade que passa ao mercado consumidor". (TJRO, Des. Marcos A. Grangeia, Rec. n. 100.007.2001.004353-1, j. 29-3-2006).

A questão é que, atualmente, independentemente de qual projeto de lei seja aprovado, qualquer lei sobre *spam* terá dificuldade de aplicação e eficácia, principalmente se buscar tipificar a conduta criminal, dada a dificuldade em provar a autoria. A determinação de guarda das provas eletrônicas, tal como manter o registro das transações de envio, que já é objeto do Substitutivo do PL 2.186, em seu art. 4º, é fundamental para tentar viabilizar a identificação de quem enviou o *spam*. Contudo, peca o referido substitutivo ao determinar que os provedores de serviço de acesso "mantenham o registro de transações de envio de grandes volumes de mensagem eletrônica". Afinal, o que seria um grande volume?

Ante o exposto, percebe-se que, apesar de ser relevante discutir no âmbito legislativo medidas para combater o *spam*, é difícil afirmar se uma lei acabará de fato com ele. O *spam* é uma praga mundial, que não se restringe apenas ao Brasil. O melhor meio para combatê-lo atualmente é: a) por meio da própria tecnologia, ou seja, por meio de programas que identifiquem e repilam o *spam*; b) pela adoção de boas práticas entre as empresas que enviam mensagem com conteúdo comercial a fim de conseguir a confiança do consumidor; c) pela denúncia, o usuário deve informar o provedor os remetentes de tais mensagens, para que tal conduta não se repita (os provedores devem disponibilizar um canal de denúncia).

Desse modo, já que no âmbito legislativo há maiores barreiras a se enfrentar no sentido de legislar sobre o tema, no tocante à autorregulamentação do mercado, o caminho é mais fácil, mais prático e mais eficaz. Para facilitar a compreensão e a implementação das melhores práticas de *e-mail marketing*, foi criado o Código de Autorregulamentação para Prática de *E-mail-Marketing* (C@PEM)²⁷⁹, de iniciativa de diversas Associações (dentre elas ABEMD,

279. Abaixo recomendações para se fazer *E-mail-Marketing* Digitalmente Correto:

- ter Política de Privacidade clara, objetiva, detalhada e publicada no *site* com barreira de navegação no cadastro;
- fazer uma gestão adequada da base de dados identificando a origem do contato e que ele tenha autorizado o envio ou se possa comprovar uma relação comercial ou social prévia (*opt-in* e *soft-opt-in*);

ABRADI, ABRANET, ABRAREC, AGADI, APADI, CGI.br, FECOMERCIO-RS, FECOMERCIO-SP, FEDERASUL, IAB, INTERNETSUL, PROTEST, SEPRORGS). O código reúne recomendações de conduta no uso de bases de dados e na forma de envio, compartilhamento e/ou exclusão de cadastros de *e-mails* para fins de *e-mail* marketing, tanto do ponto de vista técnico como jurídico e de comunicação em geral.

O Código adotou como premissa que o contato para envio de *e-mail* deve ter *Opt-in* ou *Soft-Opt-in*. No primeiro há uma autorização prévia e expressa para comunicação por *e-mail* concedida pelo destinatário ao remetente. Na segunda, apesar de não haver autorização prévia há possibilidade de comprovação de uma relação comercial ou social entre o remetente e o destinatário, inclusive motivada a partir de parcerias. Além disso, sempre deve ser assegurado o uso do recurso de *opt-out*, ou seja, a qualquer tempo o cliente pode pedir para ser excluído da base de dados, exercendo seu direito a “não informação”.

Uma inovação trazida pelo Código e que contribui para combater o *spam* é o requisito de que o remetente só possa enviar mensagens vinculados ao seu próprio nome de domínio, e não fazer uso de nomes de domínios de terceiros não pertencentes ao mesmo grupo econômico do remetente ou seus parceiros. Isso faz com que o remetente precise se preocupar em manter seu “domínio limpo” nas listas anti-*spam*. Há inclusive em seu art. 7º o detalhamento do que seria requisito para quando se faz uso de empresa parceira.

Uma polêmica resolvida também pelo Código envolve a proibição de se enviar a primeira mensagem para que solicite a autorização dos destinatários para enviar as seguintes. Este mecanismo é comumente utilizado por *spammers*, em que, de modo automatizado, envia várias mensagens, alterando o nome do remetente e fazendo com que seja “sempre” uma situação de “primeira mensagem” e sem qualquer possibilidade de *opt-out*, já que a resposta a um *e-mail*

- não usar domínios de terceiros para envio das mensagens;
- campo assunto de fácil identificação com descritivo relacionado ao conteúdo do *e-mail*;
- ter a opção de *opt-out* nos *e-mails*;
- realizar a exclusão do contato da base de dados em 2 a 5 dias úteis a partir da data de solicitação formal pelo destinatário;
- manter endereço de denúncia do tipo *abuse@xxx.com.br*
- informar no *site* situações de *e-mail* falso para evitar ser confundido com *phishing* (não conter *link* que remeta a código malicioso);
- evitar uso de palavras que gerem dupla interpretação ou tenham cunho ofensivo ou discriminatório.

spam, em vez de diminuir o seu envio, acaba por gerar a confirmação de que o *e-mail* está ativo e aí então a pessoa recebe mais *spam* ainda.

O Código vem distinguir as empresas preocupadas com a comunicação ética com seus clientes pela via digital daquelas que não estão em conformidade com as leis, as melhores práticas de mercado e a própria ética, por isso faz a exigência de que o remetente tenha uma política de privacidade formal publicada em seu *site*. Desse modo, o Código traz também uma orientação ao consumidor, com algumas diretrizes que podem o ajudar a escolher melhor para qual empresa fornecerá seus dados em seus próximos cadastros.

Independentemente do Código, devemos atender as leis vigentes. São aplicáveis os artigos do Código de Defesa do Consumidor (especialmente os arts. 43 e 44), bem como artigos do Código Civil (arts. 21, 186, 187, 927) e da Constituição Federal (art. 5º, X). Neste ano deve crescer ainda a demanda por *e-mail* de marketing político, já que com a alteração da Lei Eleitoral (Lei n. 9.504/97, alterada pelo PL n. 5.498/2009 e PLC n. 141/2009), a campanha poderá fazer uso de *e-mail* e de SMS (comunicação por mensagem de texto no celular). A lei adota o princípio do *opt-out*, em que em seu art. 57, “b”, III, prevê pena de multa de R\$ 100,00 por mensagem reincidente, tendo o prazo de até 48 horas para atender a solicitação de retirada da base.

8.40. Acessibilidade

Construir e manter um *site* na Internet significa maior alcance dos negócios da empresa. Milhões de pessoas no mundo todo podem ter acesso imediato a informações que irão auxiliar o desenvolvimento de transações, parcerias, compras e demais negócios. Um diferencial para o *site* é a utilização de recursos gráficos, como sons e animações que tornam a página mais atrativa para o visitante. Apesar de esses efeitos parecerem fascinantes para grande parte da população, um *site* pode estar passando despercebido para várias pessoas que não possuem condições físicas para enxergar, ouvir ou desfrutar de todos os recursos disponíveis. Além do aspecto lúdico, podem deixar de ser transmitidas informações úteis, induzindo o usuário ao erro ou simplesmente fazendo com que ele saia do seu *site* e visite o da concorrência.

A acessibilidade digital é o conceito que orienta desenvolvedores de *sites* a produzir conteúdos compreensíveis por pessoas portadoras de diversas necessidades especiais. Esses conteúdos são compatíveis com *softwares* específicos, que fazem a leitura de maneira compatível com a compreensão do usuário. Para

Tim Berners-Lee, diretor do W3C e inventor da World Wide Web, “o poder da *web* está em sua universalidade. Ser acessada por todos, independente de deficiência, é um aspecto essencial”.

Segundo informações do Serviço Federal de Processamento de Dados — Serpro²⁸⁰ (www.serpro.gov.br), entre as opções mais comuns para determinados tipos de deficiência estão as seguintes:

“a) Cegueira: para acessar a *web*, muitas pessoas cegas utilizam o leitor de tela²⁸¹. Alguns usuários usam navegadores textuais²⁸² como o Lynx ou navegadores com voz²⁸³, em vez de utilizar um navegador comum (navegador com interface gráfica). É muito comum a pessoa cega utilizar tecla ‘tab’ para navegar somente em ‘links’, em vez de ler todas as palavras que estão na página. Desse modo, é possível ter uma rápida noção do conteúdo da página, acessando o ‘link’ desejado mais rapidamente. Exemplos de barreiras ao acessar o conteúdo de uma página: imagens que não possuem texto alternativo; imagens complexas. Exemplo: gráfico ou imagem com importante significado e que não possuem descrição adequada; vídeos que não possuem descrição textual ou sonora; tabelas que não fazem sentido quando lidas célula por célula ou em modo linearizado; ‘frames’ que não possuem a alternativa ‘noframe’, ou que não possuem nomes significativos; formulários que não podem ser navegados em uma

280. É a maior empresa pública de prestação de serviços em tecnologia da informação do Brasil. Foi criada pela Lei n. 4.516, de 1º de dezembro de 1964, para modernizar e dar agilidade a setores estratégicos da Administração Pública. O Serpro, como Empresa cidadã de tecnologia da informação e comunicação, tem o compromisso de promover e divulgar a iniciativa da acessibilidade na Internet e desenvolver soluções com critérios de acessibilidade. Movido por esta compreensão e em sintonia com a política social e de informática do Governo Federal, o Serpro está mobilizado para encontrar soluções tecnológicas que abram caminhos para a inclusão social de milhões de cidadãos com necessidades especiais (Fonte: www.serpro.gov.br/servicos/acessibilidade).

281. “LEITOR DE TELA: *software* que lê o texto que está na tela do microcomputador e a saída desta informação é através de um sintetizador de voz ou um *display braille* — o leitor de tela “fala” o texto para o usuário ou dispõe o texto em *braille* por meio de um dispositivo no qual os pontos são salientados ou rebaixados para permitir a leitura” (Fonte: www.serpro.gov.br/servicos/acessibilidade).

282. “NAVEGADOR TEXTUAL: navegador baseado em texto, diferente dos navegadores com interface gráfica, no qual as imagens são carregadas. O navegador textual pode ser usado com o leitor de tela por pessoas cegas e também por aquelas que acessam a Internet com conexão lenta” (Fonte: www.serpro.gov.br/servicos/acessibilidade).

283. “NAVEGADOR COM VOZ: sistema que permite a navegação orientada pela voz. Alguns possibilitam o reconhecimento da voz e a apresentação do conteúdo com sons; outros permitem acesso baseado em telefone (mediante comando de voz pelo telefone e/ou por teclas do telefone)” (Fonte: www.serpro.gov.br/servicos/acessibilidade).

sequência lógica ou que não estão rotulados; navegadores e ferramentas que não possuem suporte de teclado para todos os comandos; navegadores e ferramentas que não utilizam programas de interfaces padronizadas para o sistema operacional em que foram baseados; documentos formatados sem seguir os padrões ‘web’, que podem dificultar a interpretação por leitores de tela.

b) Baixa visão: para acessar a *web*, algumas pessoas com deficiência visual parcial usam monitores grandes e aumentam o tamanho das fontes e imagens. Outros usuários utilizam os ampliadores de tela²⁸⁴. Alguns usam combinações específicas de cores para texto e fundo (‘background’) da página, por exemplo, amarelo para a fonte e preto para o fundo, ou escolhem certos tipos de fontes. Exemplos de barreiras ao acessar o conteúdo de uma página: páginas com tamanhos de fontes absoluta, que não podem ser aumentadas ou reduzidas facilmente; páginas que, devido ao ‘layout’ inconsistente, são difíceis de navegar quando ampliadas em razão da perda do conteúdo adjacente; páginas ou imagens que possuem pouco contraste; textos apresentados como imagens, porque não quebram as linhas quando ampliadas; demais barreiras, como as apresentadas para pessoas cegas, dependendo do tipo e extensão da limitação da visão.

c) Daltonismo: o daltonismo refere-se à falta de percepção a certas cores. Uma das formas mais comuns do daltonismo inclui a dificuldade de distinguir entre as cores vermelha e verde, ou amarelo e azul. Algumas vezes o daltonismo resulta em não perceber as cores. Para acessar a ‘web’, algumas pessoas personalizam as cores da página, escolhendo as cores das fontes e do fundo. Exemplos de barreiras ao acessar o conteúdo de uma página: quando a cor é usada como único recurso para enfatizar o texto; contrastes inadequados entre as cores da fonte e do fundo; navegadores que não suportam a opção para o usuário utilizar sua própria folha de estilo.

d) Deficiência auditiva: algumas pessoas surdas têm como primeira língua a de sinais e podem ou não ler e falar fluentemente uma língua. Para acessar a *web*, muitas pessoas dependem de legendas para entender o conteúdo do áudio. Pode ser necessário ativar a legenda de um arquivo de áudio, concentrar-se muito para ler o que está na página ou depender de imagens suplementares para entender o contexto do conteúdo. Os usuários também podem necessitar de ajuste no volume do áudio. Exemplos de barreiras ao acessar o conteúdo de uma página: ausência de legendas ou transcrições de áudio; ausência de imagens

284. “AMPLIADOR DE TELA: *software* que amplia o conteúdo da página para facilitar a leitura” (Fonte: www.serpro.gov.br/servicos/acessibilidade).

suplementares relacionadas, como o conteúdo do texto, que pode ter lenta compreensão por pessoas que têm como primeira língua a de sinais e não a que está escrita ou falada na página; ausência de linguagem simples e clara; requisitos para entrada de voz.

e) Deficiência física: a deficiência física ou motora pode envolver fraqueza, limitação no controle muscular (como movimentos involuntários, ausência de coordenação ou paralisia), limitações de sensação, problemas nas juntas ou perda de membros. Alguns podem sentir dor, impossibilitando o movimento. Para acessar a 'web', pessoas com problemas nas mãos ou braços podem utilizar um 'mouse' especial; um teclado alternativo²⁸⁵ cuja disposição das teclas esteja de acordo com o movimento da mão; um dispositivo tipo ponteiro fixado na cabeça ou na boca; 'software' de reconhecimento de voz ou outras tecnologias assistivas para acesso e interação. Exemplos de barreiras ao acessar o conteúdo de uma página: atividades nas quais o tempo de utilização é limitado; navegadores e ferramentas que não possuem suporte para teclado alternativo ou botões para todos os comandos efetuados por 'mouse'; formulários que não podem ser navegados com a tecla tab em uma sequência lógica.

f) Deficiência mental: as pessoas com deficiência mental podem apresentar dificuldades em processar a linguagem escrita ou oral, focar uma informação ou entender informações complexas. Para acessar a 'web', pessoas com deficiência na aprendizagem podem necessitar de diferentes modalidades ao mesmo tempo para acessar a informação desejada. Por exemplo, alguém que possui dificuldade na leitura pode usar um leitor de tela com sintetizador de voz para facilitar a compreensão do conteúdo da página, enquanto uma pessoa com dificuldade em processar a audição pode ser auxiliada por legendas para entender um áudio. Outras pessoas precisam desativar animações ou sons a fim de focar o conteúdo da página, necessitar de mais tempo ou depender de imagens para entender o que lhe está sendo informado. Exemplos de barreiras ao acessar o conteúdo de uma página: ausência de alternativas para permitir o recebimento das informações, como ausência de texto alternativo que pode ser convertido em áudio, de imagens suplementares ou de legendas para áudio; elementos visuais ou de áudio que não podem ser facilmente desligados; falta de clareza e consistência na organização das

285. "TECLADO ALTERNATIVO: é um dispositivo de *hardware* ou *software* que pode ser usado por pessoas com deficiência física. Fornece um modo alternativo de dispor as teclas, como, por exemplo, teclado com espaçamentos maiores ou menores entre as teclas. Podem também possuir travas que permitem a pressão de uma tecla por vez, teclado na tela ou outras modalidades" (Fonte: www.serpro.gov.br/servicos/acessibilidade).

páginas; uso de linguagem complexa sem necessidade; páginas com tamanhos de fontes absolutas, que não podem ser aumentadas ou reduzidas facilmente; uso de imagens trêmulas ou sinais com certa frequência de áudio que podem causar desconforto".

De acordo com as regras de acessibilidade, o *site* pode solicitar um selo que torna pública essa adequação. Tal certificação pode ser concedida pelo *Web Accessibility Initiative* — WAI (www.w3.org) ou pela Organização Acessibilidade Brasil (www.acessobrasil.org.br). A Acessibilidade Brasil também disponibiliza o "Da Silva", um avaliador em português de *sites* que indica as falhas existentes em determinado código-fonte, impossibilitando sua compreensão por pessoas especiais.

Frise-se, ainda, que o governo federal tem incentivado a acessibilidade mediante a edição do Decreto-Lei n. 5.296, de 2 de dezembro de 2004, e das Leis n. 10.048/2000 (que trata do atendimento prioritário) e n. 10.098/2000 (que dispõe, em termos gerais, sobre a promoção da acessibilidade das pessoas portadoras de deficiência ou com mobilidade reduzida). O referido decreto-lei estabelece prazo de um ano para que os *sites* da Administração Pública se ajustem às necessidades de portadores de deficiência visual.

Um exemplo de acessibilidade é o Portal da Justiça Federal, (www.justicafederal.gov.br). Nele são possíveis ajustes como contraste e tamanho de fonte. Outro exemplo é o Projeto Habilitar, do Núcleo de Computação Eletrônica (NCE)²⁸⁶ da Universidade Federal do Rio de Janeiro (UFRJ), cuja principal mentora é uma médica radióloga tetraplégica, a Dra. Lenira Luna, que comanda seu computador apenas com a voz. Também, desde 2006, os deficientes brasileiros contam com o Portal Nacional de Tecnologia Assistiva (<http://www.assistiva.org.br>), uma parceria entre a Secretaria de Ciência e Tecnologia para a Inclusão Social do MCT — Ministério de Ciência e Tecnologia —, em parceria com o ITS — Instituto de Tecnologia Social. O objetivo do *site* é aumentar a troca de informações e disseminar conhecimentos sobre as iniciativas que existem no Brasil para a pesquisa, o desenvolvimento e a aplicação de Tecnologia Assistiva. O portal foi construído de acordo com as normas de acessibilidade do governo federal. A longo prazo, o portal permitirá acesso via dispositivos móveis (computadores de mão e celulares) e terá conteúdo em inglês e espanhol, também em áudio. Citemos, ainda, o serviço

286. *Site*: <<http://www.nce.ufjf.br/>> Ver também: <<http://intervox.nce.ufjf.br/dosvoix/>> (site do programa DOSVOX para deficientes visuais) e <<http://intervox.nce.ufjf.br/motrix/>> (programa MOTRIX para deficientes motores).

oferecido pelo portal Rybená²⁸⁷, que apresenta a solução Player Rybená, por meio da qual é possível converter páginas da Internet para a Língua Brasileira de Sinais — LIBRAS.

É preciso que empreendedores vejam a acessibilidade como uma aliada na divulgação de seus negócios, captando novos clientes e divulgando amplamente os serviços de sua empresa, bem como o respeito por pessoas diferentes.

Hoje em dia é muito comum ouvir sobre projetos de capacitação pessoal e profissional mediante o uso da informática. Escolas e centros especiais são equipados e esforços são reunidos para que o cidadão faça do computador uma ferramenta de crescimento. Porém, muitas vezes os deficientes físicos são deixados de lado, pois ainda persiste a ideia de que o mundo digital seria inviável para as pessoas com necessidades especiais.

O que não é levado em conta é que a tecnologia tem melhorado — e muito — a qualidade de vida das pessoas que têm acesso a ela. Cegos que desejassem ler uma publicação estrangeira tinham de encomendar pelo correio uma cópia em Braille e aguardar sua chegada. Atualmente já é possível fazer *download* de qualquer material e imprimi-lo na hora em uma linguagem inteligível! A comunicação a distância de surdos também melhorou incrivelmente, possibilitando conversas em *chats*, *e-mails*, SMS, fóruns etc. Essa foi uma melhora significativa para quem praticamente só podia conversar de modo presencial e com quem entendesse a linguagem de sinais.

Exemplos de melhorias na qualidade de vida dos deficientes físicos e mentais não faltam. É por essa grande evolução que pessoas especiais não podem ser esquecidas por projetos de capacitação. Na visão de Marcos Kinsky, coordenador do Programa Estratégico de Acessibilidade Digital do Serpro, “o respeito à diversidade deve nortear os trabalhos de inclusão digital”. É evidente que o ensino pode ser mais caro e exigir profissionais especialmente habilitados para essa função, mas não será possível uma inclusão digital²⁸⁸ plena se questões como a acessibilidade não forem postas em prática com a importância que devem merecer.

287. Portal Rybená (página da *web* <<http://www.rybena.org.br/>> — acesso em 17-7-2008).

288. Uma referência é a Rede SACI <www.saci.org.br>, que atua como facilitadora da comunicação e da difusão de informações sobre deficiência, visando a estimular a inclusão social e digital, a melhoria da qualidade de vida e o exercício da cidadania das pessoas com deficiência.

8.41. Comunidades *online*, *blogs* e *fotologs*

O avanço tecnológico na comunicação sempre perseguiu o objetivo de criar uma “aldeia global”²⁸⁹. Na era da Internet, cada vez mais temos ampliado o poder do indivíduo, que está capacitado por meio da tecnologia a ser e estar em qualquer lugar a qualquer tempo.

Como meio de integração social, a Internet trouxe algumas inovações, fazendo com que as antigas formas de relacionamento fiquem mais dinâmicas e acessíveis em uma amplitude mundial, possibilitando um elo ainda maior entre as pessoas. Como exemplo de elementos que trazem esse benefício, podemos citar as comunidades *online* ou comunidades virtuais²⁹⁰, os *blogs* e os *fotologs*.

Comunidades virtuais acabam por ser um ponto de encontro entre pessoas com interesse em comum, sendo que algumas dessas comunidades *online* estão inseridas nas redes sociais. Para abordar a questão conceitual e dinâmica de funcionamento, nada melhor do que exemplificar com uma das comunidades mais conhecidas do momento que foi o Orkut²⁹¹. No próprio *site* podemos encontrar sua definição como sendo uma comunidade *online* de amigos, cujo principal objetivo é oferecer um ambiente que enriqueça a vida social de seus usuários.

Os recursos disponibilizados pelo até então *site* de relacionamento vão desde formas de contato *online* por mensagens chamadas de *scraps* ou ainda testemunhos, *e-mail* interno, álbum de fotos compartilhado com amigos, possibilidade de rastrear os amigos que estão ligados a outros amigos de seu círculo de conhecidos, e até mesmo participar de comunidades internas, que seriam subcomunidades dos mais diversos interesses.

289. “O conceito de ‘aldeia global’, criado pelo sociólogo canadense Marshall McLuhan, quer dizer que o progresso tecnológico estava reduzindo todo o planeta à mesma situação que ocorre em uma aldeia. Marshall McLuhan foi o primeiro filósofo das transformações sociais provocadas pela revolução tecnológica do computador e das telecomunicações” (disponibilizado na Wikipédia — página da *web* <http://pt.wikipedia.org/wiki/Aldeia_global> — acessado em 17-7-2008).

290. A expressão “comunidade virtual” ganhou força nos últimos tempos, principalmente por conta do sucesso do Orkut em todo o mundo e especialmente no Brasil. Mas o que pouca gente sabe é que esse conceito é mais antigo do que a própria Internet e muito mais amplo do que Orkut e coisas semelhantes. O pesquisador Howard Rheingold, que em 1993 previu que a Internet e o universo virtual provocariam grandes mudanças para o homem do século XXI, escreveu diversos livros sobre Internet, novas tecnologias e, é claro, comunidades virtuais. (Fonte: Wnews.)

291. Site: <<http://www.orkut.com>>.

Criada pelo turco Orkut Buyukkokten, o Orkut se tornou um espaço para grupos promoverem apologia a crimes²⁹², ofensas, *bulling*, entre outros. Não podemos esquecer que muitas das criações e inventos do ser humano foram idealizados para o melhor, mas tudo que se cria para o bem, acaba muitas vezes sendo utilizado também para o mal.

Com o passar do tempo, outras redes sociais ganharam mais destaque, principalmente o *Facebook*, por possuir muito mais recursos de interação do que o *Orkut*. Além disso, é a maior rede social do mundo. O *Twitter* também é outra rede social que possui vários adeptos, na forma de “microblog” cada *tweet* é caracterizado pela sua instantaneidade e pelo limite de cento e quarenta caracteres. Ambos possuem políticas de uso e privacidade específicos que devem ser observados pelos usuários, sob pena de terem suas “vidas *online*” excluídas.

É comum os usuários terem a falsa impressão de que somos completamente livres quando estamos *online*, e que a nossa conduta neste ambiente não é alcançada pela lei²⁹³, ou seja, acham que o virtual não pode se tornar real. Pensam ainda que estão totalmente anônimos. Assim, falsidade ideológica, calúnia, difamação, injúria, racismo, ameaça, violação de direito autoral, divulgação de segredo, violação de segredo profissional, tráfico de drogas, apologia de crime ou criminoso e formação de quadrilha ou bando são apenas alguns exemplos de crimes livremente praticados no *website*²⁹⁴.

292. Ver mais em <<http://www.denunciar.org.br/twiki/bin/view/SaferNet/Noticia20060313113124>>. Autor: Bruno Gilliard, publicado no Jornal *Bom Dia*.

293. O Ministério Público Federal em São Paulo entrou com uma ação junto à Justiça Federal no dia 16 de março de 2006, pedindo a quebra de sigilo do Orkut, serviço de comunidades virtuais do Google. A quebra de sigilo envolve tanto criadores como usuários brasileiros de comunidades virtuais usadas para práticas criminosas. O mesmo acordo foi firmado com alguns provedores de acesso à Internet em novembro do ano passado. No dia 10 de abril de 2006, o diretor-geral do Google Brasil compareceu a uma audiência no MPF para esclarecer o envolvimento de mais de 5 mil brasileiros em comunidades no Orkut que praticam crimes como racismo, tráfico de drogas, distribuição de materiais de pornografia infantil, distribuição de receitas médicas em branco, de medicamentos controlados sem receita médica, entre outros. As informações foram coletadas em um dossiê de 150 páginas elaborado entre a segunda quinzena de dezembro de 2005 e janeiro de 2006 pela SaferNet (<http://www.denunciar.org.br>), organização sem fins lucrativos que combate crimes contra os direitos humanos na grande rede. Ver em <<http://www.denunciar.org.br/twiki/bin/view/SaferNet/Noticia20060313113124>>. Autor: Bruno Gilliard, publicado no Jornal *Bom Dia*.

294. Em janeiro de 2006, o governo americano moveu uma ação na Corte para impelir o Google, responsável pelo Orkut, a cumprir com a intimação emitida no ano de 2005 de entregar os dados de sua base, por meio de uma “amostra randômica”, de 1 milhão de endereços disponíveis no mecanismo. Os dados deveriam contribuir para a defesa de uma legislação chamada Ato de Proteção Online das Crianças (Child Online Protection Act — COPA), que vem sendo

Segundo a Dra. Cristina Sleiman, “a palavra ‘blog’ surgiu da abreviação de ‘weblog’, sendo que *web* refere-se e à Internet e ‘log’ significa diário de bordo. Originalmente é um documento oficial utilizado em navios e aviões, para relato de informações importantes. Por um aspecto virtual, o ‘blog’ foi definido como um diário ‘online’, publicado na internet e atualizado com frequência. Nele pode se expor opiniões de qualquer assunto e postar textos provenientes de qualquer conteúdo”²⁹⁵.

Atualmente, o *blog* é mais do que um diário. Muito utilizado por jornalistas e empresas acabou por tornar-se uma poderosa forma de comunicação. Tal ambiente permite ainda a coautoria, pois várias pessoas podem ter permissão de edição e publicação.

As publicações são feitas de forma cronológica, facilitando o acesso a determinadas publicações seja qual for o período.

O *blog* permite ainda a interação com seus leitores, ou seja, é possível uma terceira pessoa deixar uma mensagem para o “dono”, autor do *blog* e este, por

questionada nos tribunais pela União das Liberdades Cívicas da América (American Civil Liberties Union — ACLU). Ver <http://www2.metodista.br/unesco/jbcc/jbcc_mensal/jbcc280/jbcc_estado_eua_buscadores.htm>. Em uma decisão já antecipada, um juiz federal dos Estados Unidos determinou, dia 17 de março de 2006, que o Google deve entregar ao governo dados sobre o índice da sua ferramenta de busca, mas não precisa enviar a amostra das buscas realizadas por usuários na sua base. Ver <<http://idgnow.uol.com.br/internet/2006/03/20/idgnoticia.2006-03-20.6559309097>>.

Casos de danos à imagem de marcas acontecem no Brasil cada vez mais nas redes sociais, como ocorreu com uma marca de calçados que utilizou pele animal na fabricação de seus sapatos e bolsas, e gerou grande repúdio nas grandes redes sociais e isso fez com que a linha fosse retirada de comercialização. Disponível em: <<http://www.opovo.com.br/app/maisnoticias/brasil/2011/04/18/noticiabrasil,2129353/apos-protestos-nas-redes-sociais-arezzo-decide-recolher-colecao-pelemanias.shtml>>.

A Secretaria de Cultura do Estado de São Paulo “postou” no seu perfil oficial no Twitter que lamentava a morte do ex-Vice Presidente da República José de Alencar, perguntando por que, em vez de Alencar, não poderia ter falecido o Sarney: “Por que foi o José Alencar e não o #Sarney?”. Em seguida da gafe, a Secretaria da Cultura apagou a mensagem e pediu desculpas pelo ocorrido. Disponível em: <<http://noticias.uol.com.br/politica/ultimas-noticias/2011/03/29/por-que-foi-o-jose-alencar-e-nao-o-sarney-diz-secretaria-de-cultura-de-sao-paulo-no-twitter.htm>>.

Há problemas não só relacionados a marcas, mas também à reputação da própria pessoa. Houve o caso de uma estudante de Direito, na época das eleições presidenciais, que utilizou o Twitter para xingar os nordestinos. O caso gerou grande repercussão e a garota teve que deixar a faculdade onde estudava e o trabalho, além de estar sendo processada pelo crime de racismo. Disponível em: <<http://idgnow.uol.com.br/internet/2011/12/12/ministerio-publico-aceita-denuncia-e-mayara-petruso-respondera-por-racismo/>>.

295. SLEIMAN, Cristina M. Utilização das Novas Tecnologias de Informação e Comunicação no Senac São Paulo. 4ª Conferência Ibero-Americana em Sistemas, Cibernéticas e Informática. 2005. Orlando, FL.

sua vez, tem obrigação de promover sua gestão de forma lícita, ou seja, ao tomar conhecimento de mensagens ofensivas, deve eliminá-las imediatamente, sob pena de ser responsabilizado. Exemplo prático foi o caso do *blog* Imprensa Marrom, que segundo notícia publicada por diversas empresas de comunicação, foi condenado a pagar R\$ 3.500,00 (três mil e quinhentos reais) ao ofendido, após se recusar a retirar um comentário em nome da liberdade de expressão. Cabe mencionar que a Internet possui hoje mais de 20 milhões de *blogs*.

Os *photoblogs* são ambientes virtuais que permitem a publicação de fotos e muitas vezes também de mensagens. Alguns serviços deste tipo oferecem também fóruns de discussão.

Podemos perceber que todos os ambientes virtuais citados acima são passíveis de condutas indevidas. Portanto é preciso uma análise sob quatro aspectos de gestão de risco: segurança da informação/criminalidade; consumidor/relacionamento; uso não autorizado de marca e produtividade. Para cada um dos aspectos há uma medida mais adequada para minimizar os riscos e gerenciar o uso dessa nova ferramenta de comunicação.

É preciso atenção ao utilizar tais mídias, uma vez que as novas formas de expressão e linguagem surgidas com os *blogs* e comunidades virtuais devem estar adequadas não apenas aos princípios gerais do Direito, mas também às boas práticas legais, para que algo que deveria ser uma diversão, uma opinião ou uma comunicação não se transforme num Boletim de Ocorrência ou ação judicial.

As leis tratam de condutas, não importa se físicas, orais ou eletrônicas, ou seja, valem as regras para qualquer meio, inclusive para a Internet. Ao receber um *e-mail* afirmando que alguém é isso ou aquilo e repassá-lo adiante, o usuário pode também assumir a responsabilidade por possível dano moral ou material. Pode até mesmo estar cometendo um crime, sendo o mais comum o de difamação, previsto no art. 139 do Código Penal brasileiro. É importante ressaltar que essas ações não estão amparadas pela liberdade de expressão. São infrações!

Ademais, deve-se ter especial atenção com o uso de imagens, questão relacionada ao direito à privacidade, protegido pela Constituição Federal de 1988, conforme está regulamentado em seu texto, no art. 5º, X, o qual afirma que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Idêntico cuidado merece ser observado em relação à inserção de textos ou conteúdos por terceiros, uma vez que o proprietário do *blog* ou comunidade é responsável por aquilo que é publicado em sua página, assim como no exemplo utilizado anteriormente neste capítulo sobre o *blog* Imprensa Marrom. A informação deve ser retirada do ar ao menor indício ou notificação de que possa gerar lesão a alguém²⁹⁶, ser falsa, ou ser contra os bons costumes, sob pena de ser considerada responsabilidade por omissão²⁹⁷.

Conforme consta no texto da Declaração dos Direitos do Homem e do Cidadão, aprovada pela França em 26 de agosto de 1779, “a liberdade consiste em poder fazer tudo o que não prejudica o outro, de modo que os únicos limites do exercício dos direitos naturais de cada homem são aqueles que garantem aos outros membros da sociedade o gozo desses mesmos direitos; esses limites só podem ser determinados pela lei”.

No âmbito digital, tudo o que está *online* é uma evidência, uma possível prova que pode ser usada contra a pessoa. Há coisas na vida que devemos apenas pensar; existem outras que podem ser faladas, escritas, ou publicadas.

No tocante a recomendações e boas práticas para uso de *blogs* e comunidades, é fundamental ressaltar que na era da Internet também vale o princípio do “diga-me com quem andas que eu te direi quem és”, ou seja, quando um internauta se cadastra para integrar uma comunidade *online*, como a do Orkut, ele passa a assumir que concorda, mesmo que tacitamente, com o conteúdo dela, quer seja o que ele mesmo tenha dito ou o que seja dito por outros integrantes. Há algumas hipóteses que podem ocorrer:

296. Fundamentos nos seguintes artigos do Código Civil: “Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”; “Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes” e “Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo”.

297. “O governo tomou providências para retirar da Internet a página no orkut do ministro chefe da Secretaria de Comunicação de Governo e Gestão Estratégica, Luiz Gushiken. Também saiu do ar a página da mulher do presidente, Marisa Leticia Lulinha da Silva”. A ordem foi executada pela Abin — Agência Brasileira de Inteligência. O governo alega que as páginas eram falsas. Além das comunidades em torno do secretário de comunicação e da primeira dama, navegam pela rede de computadores outros orkuts em nome do ministro da Fazenda, Antônio Palocci, do ministro da Integração, Ciro Gomes, e outras autoridades do primeiro escalão da República. O que é verdadeiro e o que é falso fica difícil de saber. No caso do orkut de Gushiken, uma leitura atenta de sua biografia revela uma incongruência logo na primeira linha: ‘Sou o ministro chefe da presidência de Luís Inácio Lula da Silva’. Não só o nome do presidente se escreve com ‘z’ como não existe o cargo de ministro chefe da presidência” (Fonte: Revista Consultor Jurídico. Notícia publicada em 1º-5-2008 — disponível na web página <<http://www.conjur.com.br/static/text/33899,1>> — acessado em 18/7/2008).

1ª) O internauta é o dono da comunidade, *blog* ou fórum que foi criada já com um tema ilegal, como venda de drogas, conteúdo difamatório, racial, com nome de marcas de empresas, com nome de pessoas e imagens sem autorização. Nessa situação, o dono, no caso gestor do ambiente, é o infrator principal.

2ª) O internauta é mero integrante da comunidade, fórum ou leitor participante de *blog*, ou seja, aquele que publica seus comentários em ambiente que trata de tema considerado ilegal ou um ilícito civil, autoral ou criminal. Nesse caso, ele pode ser envolvido em uma investigação para averiguar se ele é coautor, partícipe, facilitador etc., ou seja, ele pode ser responsabilizado.

3ª) O internauta é integrante da comunidade, fórum ou participa de algum *blog* que é correto, é legal, mas ele escreveu textos ilegais, ofendeu terceiros ou cometeu outros ilícitos dentro da Comunidade. Ele será o responsável e será considerado o infrator. Mas, se houver uma notificação ao dono da comunidade sobre o conteúdo lesivo, e ele não tirar do ar, passa a ser coautor também, assim como os demais integrantes poderão vir a ser envolvidos, dependendo da análise do contexto, dos conteúdos, das participações de cada um, caso a caso.

O uso de imagens é questão relacionada ao direito à privacidade, protegido pela Constituição Federal de 1988. É necessário ter especial atenção com o uso delas, uma infração nos meios eletrônicos deixa vários vestígios.

Como dito, tudo o que está *online* é uma evidência, uma possível prova que pode ser usada contra a pessoa. Seguem, portanto, algumas dicas para quem quer navegar sem riscos:

- Dê sempre o crédito de fotos e textos, áudios e vídeos, mesmo que os autores sejam “anônimos” ou “desconhecidos”. É fundamental fazer a citação da fonte ou do autor para evitar infringir a Lei.

- Se não for possível obter a autorização prévia do autor para publicação na Internet do conteúdo, então se deve limitar a disponibilizar até 1/4 da obra, segundo melhores práticas internacionais (observando que isso ainda não está previsto na legislação brasileira, é uma prática de costumes).

- Nunca publicar na comunidade *online* textos ou imagens que possam ser ofensivos, pois pode configurar crime de difamação ou calúnia, além de responsabilidade civil. É importante apurar a veracidade dos fatos antes de divulgá-los, pois a pessoa passa a assumir o conteúdo que publica, mesmo que seja de terceiros. Consulte *sites* especializados, como o E-farsas²⁹⁸, que desvenda as histórias que circulam pela rede.

298. Disponível na *web* em <<http://www.e-farsas.com/>>.

- Nunca divulgar informações confidenciais da empresa em que o dono da comunidade ou do comentário trabalha. Pedir sempre autorização para falar em nome de seus empregadores.

- Nunca divulgar *banners* para *sites* pornográficos, pois pode ser enquadrado como um meio de favorecimento à prostituição.

- Não criar comunidades com temas ilegais ou que atentem aos bons costumes, tais como drogas, pornografia, pedofilia, ensinando a fazer ligações clandestinas de serviços, cópias ilegais de produtos ou *softwares*, ou qualquer outro ato ilícito.

- Não publicar imagens que possam configurar atos obscenos, pois pode ser configurado crime, a teor do art. 234 do Código Penal. Nem “aquele dedo”, nem mesmo sendo o seu.

- Somente publicar fotografias com uma condição: com autorização do fotógrafo e das pessoas que aparecem na imagem. As imagens não podem ser obscenas e ofensivas.

- Não utilizar termos que possam ser considerados racistas, criticando alguém por causa de sua cor, pois é um crime muito grave.

- Usar somente logomarca e nome de empresas mediante autorização do titular.

- Não montar comunidades com nome de outras pessoas, nem com conteúdos prejudiciais a ela, pois pode gerar um processo de indenização por danos morais e materiais, bem como processo criminal.

- Não se passar por outra pessoa, divulgando seus dados e informações (verdadeiras ou não) sobre sua vida. Isso configura crime de falsa identidade ou de inserção de dados falsos em sistema de informação.

- Comunicar a empresa que hospeda a comunidade quando algum usuário postar comentários ilegais ou que vão de encontro aos termos de uso do serviço.

- Se você é o responsável e titular da comunidade, e ao receber uma notificação de que algum conteúdo publicado é ofensivo, ou fere direitos de terceiros, retire-o imediatamente do ar, para não ser considerado coautor.

- Não passar para a frente boatos eletrônicos.

A questão da educação das novas gerações é essencial. Muito tem sido estudado sobre como orientar os jovens no uso ético, seguro e legal da Internet e das novas mídias²⁹⁹.

299. Para saber mais ver o *blog* da Dra. Cristina Sleiman <<http://edigital.zip.net/>>, <[355](http://</p></div><div data-bbox=)

8.42. Internet móvel

A Internet móvel vem atender às necessidades do surgimento de uma sociedade com iguais características, em que os indivíduos se deslocam o tempo todo e carregam a possibilidade de ser identificados e localizados eletronicamente a qualquer momento. Para melhor elucidar a complexidade desse modelo móvel de relacionamento, vamos tomar o exemplo prático da Finlândia, hoje um dos países em que a telefonia móvel está mais evoluída no mundo — as próprias dificuldades geográficas de montar conexões por cabo terrestre naquele país forçaram esse desenvolvimento. Há uma média altíssima de dois telefones celulares por habitante finlandês; na prática, isso significa que muitos dos finlandeses carregam até três aparelhos simultaneamente. Por quê? Porque a Finlândia é hoje um espelho do que será a sociedade móvel em outros países do mundo dentro de algum tempo — uma sociedade móvel em que o celular é um instrumento básico que possibilita desde comprar um refrigerante em uma máquina (digita-se determinado código usando o celular e a operação é efetuada, tendo seu custo debitado na conta telefônica) até fazer as mais intrincadas operações bancárias. Muitas pessoas terão mesmo mais de um aparelho, pois desejarão ter mais de uma identidade eletrônica, separando aquela identidade usada para o cotidiano do trabalho da utilizada para o cotidiano familiar e desta para o pessoal (como muitos de nós optamos por ter várias identidades financeiras — por exemplo, uma conta corrente individual, outra ligada à empresa em que trabalhamos, outra em conjunto com nosso cônjuge etc.).

A Sociedade Digital Móvel traz acessibilidade vinte e quatro horas por dia aos seus membros, mesmo quando em deslocamento. Essa funcionalidade pode ser vantajosa, mas ao mesmo tempo é um pouco aflitivo pensar que “alguém” pode saber por onde você andou durante todo o tempo e o que fez. Mais uma vez, estamos diante de uma situação de confronto entre segurança e privacidade.

Todas as questões analisadas no âmbito de privacidade, publicidade e comércio eletrônico tomam um caráter muito mais delicado, já que a mobilidade através de dispositivos traz uma capacidade de individualização muito maior que os outros mecanismos de comunicação, como TV, rádio, telefone e

blog.aprendaki.com.br/entrevista_ver.asp?id=64>, <<http://www.denunciar.org.br/twiki/bin/view/SaferNet/Noticia200609013022526>>, <<http://br.buscaeducacao.yahoo.com/mt/archives/2006/07/responsabilidad.html>>, <http://www.educarede.org.br/educa/index.cfm?pg=internet_e_cia.informatica_principal&id_inf_escola=652>, <http://www.educarede.org.br/educa/internet_e_cia/informatica.cfm?id_inf_escola=240>.

computador. Seja por celular, por *palm top*, pelo *videogame*, pela geladeira ou por qualquer outra interface de contato, o consumidor tem a capacidade de ser identificado com uma precisão muito maior, assim como de estabelecer uma relação comercial imediata.

O comércio eletrônico móvel, ou *m-commerce* (abreviação para *mobile commerce*), cria um novo aspecto jurídico de responsabilidade e obrigações, já que a empresa de telecomunicação passa a ser responsável pelo repasse do valor pago pela compra de produtos via telefone celular — seja ele comprado na navegação pela Internet ou por uma transação eletrônica remota (como no exemplo da máquina de refrigerante).

As possibilidades de serviços de valor agregado são muitas. Um celular, por exemplo, pode servir como localizador GPS, para o caso de prevenção a sequestros, para acionar um socorro médico emergencial, podendo estar em sintonia, por exemplo, com um marca-passo e acusar para o médico qualquer disfunção interna do organismo que possa estar ocorrendo sem que o paciente nem sequer saiba.

Quanto à publicidade, a questão da Mídia Responsável e da Mídia de Resultado fica ainda maior, já que os cuidados quanto à permissão do usuário para receber publicidade devem ser muito grandes, para não lesar seu direito à privacidade.

Com a convergência da TV com o telefone, temos o primeiro veículo audiovisual *broadcast* interativo de comunicação individual, não mais de massa. E isso, por certo, já faz com que os direitos autorais de imagem, de artistas, de conteúdos e programas interativos para *broadcast* móvel tenham de ser repensados em termos contratuais, assim como os contratos de anunciantes, da mídia e da própria compra e venda móvel, entre outros.

Há muito que estudar sobre essa nova evolução trazida pela mobilidade, mas, certamente, muitas das soluções aplicáveis serão as mesmas que as já encontradas para as operações na *web*.

8.43. TV Interativa e TV Digital

A “caixa mágica”. Este foi o termo usado no lançamento da televisão no mercado³⁰⁰. O termo definia a possibilidade de ter o mundo em sua casa, den-

300. Segundo matéria divulgada pelo jornal *Estado do Paraná*, em 5-7-2006: “A televisão está presente em mais de 90% das moradias brasileiras, segundo a última PNAD — Pesquisa

tro de uma caixinha preta. A revolução causada pela TV levou mais de trinta anos até que conseguisse estabilidade como um veículo de mídia. A Internet levou bem menos tempo. Como no caso da Internet, o Brasil foi um dos primeiros países a adotar aquele veículo. Em 1950, Assis Chateaubriand inaugurava a primeira emissora do País, embora nossa estrutura de transmissão e a própria realidade social estivessem muito aquém do progresso representado pela TV. De qualquer forma, o pioneirismo de Chateaubriand fez com que o Brasil se tornasse um dos países em que as tecnologias de comunicações encontrariam grande espaço para expandir-se. Com a chamada TV Interativa, não será diferente: em pouco tempo, estaremos convivendo, como a maioria dos países de ponta, com um novo e revolucionário veículo.

Junto com a revolução da TV, criou-se uma avalanche de normas sobre telecomunicações e radiodifusão, com suas concessões, licenças específicas, contratos *broadcast*, de transmissão, de programação, de conteúdo, entre outros. Naqueles primórdios, muitos achavam que os jornais e revistas iriam acabar. A história, entretanto, mostra que as novas tecnologias de comunicação não fazem desaparecer as anteriores, ao contrário, contribuem para reforçá-las, como o que ocorreu com o crescimento e amadurecimento de toda a indústria impressa.

A Televisão Interativa, ou "ITV", por sua vez, traz uma tecnologia revolucionária, em que o telespectador pode realmente interagir com sua televisão, tendo direito a uma programação personalizada, com aquilo que ele quer assistir, quando quer e como quer. E mais, o telespectador pode estar não apenas em contato com o mundo, mas colocar o mundo em contato com ele, tornando-se acessível, conhecido como indivíduo e não mais como massa.

O principal aspecto jurídico a ser examinado no tocante à ITV está relacionado aos direitos autorais, uma vez que os contratos com artistas, autores, escritores, roteiristas, produtoras de vídeo, produtoras de conteúdo devem prever não apenas determinada quantidade de exibições *broadcast* ou entradas na programação, como também a quantidade de *downloads* específicos da programação personalizada do telespectador, que não necessariamente acompanham o estabelecido na programação tradicional³⁰¹.

Nacional por Amostra de Domicílios — divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), o que representa mais de 50 milhões de aparelhos analógicos espalhados pelo País". Ver em <http://www.mackenzie.com.br/dhtml/assessoria_comunicacao/imprensa/macknaimprensa.php?ano=2007&ass=1234>.

301. De acordo com a Lei n. 9.610, de 19 de fevereiro de 1998, que consolida a legislação sobre direitos autorais, depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades, como a radiodifusão sonora ou televisiva (art. 29). O mesmo diplo-

Uma solução adequada dentro dos critérios já analisados de Direito Digital consiste na adoção de sistemas de pagamento pelo telespectador em que determinada porcentagem pode já estar previamente estabelecida em contrato para ser destinada aos sindicatos, artistas, autores, diretores, produtoras etc. Estamos falando da adaptação da tecnologia *pay-per-view* para ser aplicada no *pay-per-use*, *pay-per-download*, *pay-per-play*. Isso atende não só aos conteúdos *broadcast*, como também aos conteúdos interativos, jogos, *softwares* que podem ser baixados através da ITV, o *video-on-demand*, entre outros.

Com a transmissão digital, o aparelho de TV deixa de ser um terminal passivo e passa a oferecer ao usuário a possibilidade de interagir com o conteúdo. Os aparelhos receptores — sejam televisores digitais ou conversores — possuem capacidade de processamento local, transformando-se em variações do computador. Como benefícios diretos proporcionados pelo uso da TV Digital, podemos destacar a disponibilidade do uso de aplicativos, a interatividade, a prática de comércio eletrônico, a mobilidade, a qualidade da transmissão/recepção de áudio e vídeo.

No mundo, existem três padrões de distribuição digital de sinais: Advanced Television Standard Committee (ATSC), o padrão norte-americano, adotado pelos Estados Unidos, Canadá, México, Coreia do Sul e Taiwan; Digital Video Broadcasting — Terrestrial (DVB — T), que é o padrão chamado europeu, escolhido por Reino Unido, Itália, Suécia, França, Portugal, Espanha e Alemanha, além da Austrália e de Cingapura; e, finalmente, o padrão Integrated Services Digital Broadcasting — Terrestrial (ISDB), em uso no Japão. No Brasil, o governo decidiu realizar uma pesquisa para ter sua própria tecnologia para a TV Digital³⁰², com o objetivo de escolher o padrão mais adequado à nossa realidade, uma vez que somos um país menos desenvolvido³⁰³.

ma ainda garante que, em qualquer modalidade de reprodução, a quantidade de exemplares será informada e controlada, cabendo a quem reproduzir a obra a responsabilidade de manter os registros que permitam ao autor a fiscalização do aproveitamento econômico da exploração (art. 30, § 2º). Sobre obras audiovisuais o legislador, protegendo os interesses dos outros coautores, além do produtor, prevê que, para os casos em que a remuneração destes esteja vinculada à utilização econômica da obra, o produtor deverá prestar contas semestralmente aos coautores (art. 84). Além dos já citados artigos, outros existem na referida lei (arts. 61 e 94) que traduzem perfeitamente a intenção do legislador, de que é devida aos autores e coautores uma participação nos rendimentos advindos de cada exibição, transmissão ou reprodução da obra.

302. <http://www.mc.gov.br/005/00502001.asp?ttCD_CHAVE=8880> do Ministério das Comunicações (2006).

303. "Todo o debate em torno da definição do padrão que servirá de modelo para o Sistema Brasileiro de TV Digital (SBTD) não é em vão. A transição para o padrão digital deverá movimentar aproximadamente 7 bilhões de reais, segundo estimativa do Centro de Pesquisa e Desenvolvimento em

Mas, enquanto o Brasil discute a adoção e implantação de seu padrão de TV Digital, a Europa já debate o padrão para a TV Digital móvel. São dois os candidatos: o T-DMB, baseado na tecnologia Digital Audio Broadcasting (DAB), já bastante utilizada no continente, e o Digital Video Broadcasting-Handheld (DVB-H), com o apoio da Nokia, Motorola, NEC e Sony Ericsson. Outra preocupação jurídica está relacionada ao potencial comercial, ou seja, da capacidade de venda de produtos e serviços pela televisão, por meio de comércio eletrônico, conhecido por “*t-commerce*” (abreviação de *television commerce*). Esta modalidade é uma fusão do contrato de mídia com um contrato de “cliques”, ou seja, a Mídia de Resultado. Nesse aspecto, ressaltamos novamente o cuidado com a Publicidade Invasiva, uma vez que a proteção à privacidade está acima dos interesses comerciais dos anunciantes.

Para aumentar a complexidade, há o fornecimento de serviços como o de *home banking* pela TV, de seguro, de compra de passagens. Isso, associado ao uso de cartão de crédito e ao fato de que uma TV pode muitas vezes atender a vários integrantes de uma mesma família ou moradores de uma mesma casa, faz com que as preocupações com segurança e quanto ao uso de informações, cadastros e bancos de dados tenham de ser ainda maiores.

Há um aspecto relevante particular dessas tecnologias: o cuidado do veículo com a corresponsabilidade por publicidade enganosa, prevista no art. 37 do Código de Defesa do Consumidor. Veja que ele já não é mero intermediário de imagens e sons — é intermediário de operações comerciais, ou seja, leva

Telecomunicações (CpQD). Desse montante, 5 bilhões de dólares correspondem ao valor que será investido pela população na aquisição de aparelhos conversores — os chamados set-top boxes — e de TVs digitais. Além disso, será investido 1,5 bilhão de reais na substituição dos sistemas de transmissão e outros 500 milhões de reais na digitalização dos estúdios das emissoras de TV. Mundialmente, o mercado de televisões digitais deve movimentar 23 bilhões de dólares em 2006, totalizando 18 milhões de receptores digitais vendidos no ano, segundo a Associação de Eletrônicos de Consumo dos Estados Unidos. Em 2005, as vendas de aparelhos cresceram 60%, atingindo 17 bilhões de dólares. Segundo projeções do Instituto de Pesquisas Informa, até o ano de 2010 o número de residências com televisão de alta-definição — aptas a receber o sinal digital sem necessidade de conversor — no mundo aumentará para 106,2 milhões, dos atuais 28,6 milhões. Os Estados Unidos terão o maior número de domicílios equipados — 48,3 milhões —, seguidos pelo Japão (19,9 milhões), China (10 milhões), Alemanha (5,3 milhões) e Canadá (4,3 milhões). Até o ano de 2009, os Estados Unidos pretendem ter encerrado as transmissões analógicas, o que significa que qualquer pessoa que queira assistir à televisão terá de possuir um equipamento de recepção de sinal digital. Em 2007, praticamente não serão mais vendidas TVs analógicas nos Estados Unidos, projeta Robert Graves, presidente do conselho do Fórum ATSC. No Brasil, o prazo estimado para a transição para o modelo digital é de até 15 anos, segundo o ministro das Comunicações Hélio Costa, o que significa que até 2021 ainda teremos transmissões analógicas coexistindo com as digitais” (Fonte: reportagem de autoria da repórter Daniela Moreira, disponível na web <<http://idgnow.uol.com.br/telecom/2006/02/13/idgnoticia.2006-02-13.9898766813/>>).

o telespectador do desejo à compra efetiva, por meio de alguns “cliques”. Tem de estar muito claro nos contratos de mídia, assim como para o telespectador, até onde o veículo está comprometido com as informações dos produtos e com o estímulo à compra efetiva de determinado produto causada pela estratégia de *marketing* e comercial do *software* interativo da TV.

É importante ressaltar que, no *broadcast* tradicional, o veículo televisivo não é responsabilizado pelo conteúdo dos comerciais inseridos em sua grade de programação. No entanto, novas tecnologias trazem novas complexidades jurídicas. Uma vez possibilitada a interatividade e estimulado o *t-commerce*, o veículo passa a ter uma característica jurídica diferenciada, para fins de responsabilidade. Assim, o veículo passa a ser quase que um corretor, comissionado em virtude do grau de participação e fechamento de negócios por meio de sua mídia. Ou seja, audiência tradicional não é o mesmo que audiência participativa e interativa.

Quanto aos serviços de valor agregado, como o de *t-banking*, ou seja, o banco na televisão, há que estar muito bem definido para o consumidor³⁰⁴, cliente do banco e assinante da TV, de quem é a responsabilidade, principalmente no tocante à segurança da operação³⁰⁵, e qual o seguro que dá cobertura contra fraudes, furtos etc. Assim como para os provedores de internet é recomendada manutenção dos dados de registro e arquivamento das conexões IP³⁰⁶ ocorridas no servidor e seus horários, para fins de investigação quanto a determinada ocorrência na rede, algo similar deve ser feito com a TV Interativa, uma vez que passa a ser um veículo bidirecional com fluxos de informações e dados que permitem saber quem fez, o que fez, quando fez.

304. É importante que os bancos disponibilizem para clientes que usam de seus serviços através da TV Interativa canais de comunicação entre estes e as instituições. Os Serviços de Atendimento ao Consumidor (SACs) têm esse escopo e a capacidade de resolver conflitos sem a necessidade da via judicial; a criação deles é fundamental, então, para que o consumidor se sinta mais seguro e para harmonizar as relações cliente-banco.

305. Junto com as novas tecnologias surgem aqueles capazes de identificar suas deficiências e explorá-las para fins ilegais. Será que não devemos esperar uma nova safra de *hackers* que consigam realizar transações bancárias como se outras pessoas fossem? Lembremos, como já dissemos anteriormente, que os desenvolvedores de sistemas digitais têm de investir, e muito, no quesito segurança, porque este é ainda um dos maiores entraves (para não dizer o maior) a uma adesão mais significativa da população à utilização das novas soluções em serviços da nova era digital.

306. O Projeto de Lei n. 3.891, de 2000, do Deputado Julio Semeghini, dispõe sobre o registro de usuários pelos provedores de serviços de acesso a redes de computadores, inclusive à Internet, sendo uma de suas disposições a obrigação dos provedores de serviços da Internet manterem registros de seus usuários e dados referentes a cada transação atendida pelo provedor, para solucionar o problema da identificação do usuário em caso de utilização ilícita da rede, cometida, em geral, por *hackers* ou *crackers*.

Estas são apenas algumas das situações que juridicamente já estão sendo observadas. Há muitas outras cujo nível de complexidade não nos permite descrever aqui, devido ao grau de seu detalhamento técnico que não vem ao caso, mas sabemos que nossa responsabilidade como pensadores do Direito é estar sempre trazendo soluções para a crescente complexidade das relações humanas em uma sociedade digital. Quanto mais claras todas essas questões jurídicas e de responsabilidade, mais facilmente a tecnologia será aceita pelo consumidor.

8.44. VoIP

Primeiramente, o VoIP (sigla para *voice over IP*) é o sistema de comunicação por voz baseado em IP. Para entender VoIP é preciso compreender que a comunicação na Internet se estabelece a partir de um protocolo. O termo deriva do grego *protocollon* (uma folha de papel colada a um manuscrito que descrevia seu conteúdo) e em tecnologia da informação a palavra descreve um conjunto de regras que permite o intercâmbio de informações entre pontos conectados de redes de comunicações.

Os protocolos recebem padronização internacional de acordo com o seu uso industrial. O conjunto de padrões que permite a entrega de dados entre dois sistemas conectados à Internet recebe o nome de *Internet Protocol* — IP, que juntamente com outro protocolo, o *Transmission Control Protocol* — TCP/IP possibilita a “conversa” entre estes mesmos sistemas.

Tecnicamente, VoIP vem a ser a entrega da voz digitalmente em pequenos pacotes de comunicação em vez dos tradicionais protocolos de circuitos comutados presentes em sistemas de *Public Switched Telephone Network* — PSTN, redes públicas das operadoras de telefonia outorgadas por órgão competente.

Os tipos de comunicação de Voz sobre IP mais tradicionais são: PC a PC, telefone a telefone e PC a telefone (seja fixo ou celular). Os PC's e os telefones devem estar preparados para esse tipo de comunicação, com programas e interfaces específicas previamente instalados. O usuário individual pode utilizar Voz sobre IP (VoIP) para uma conversa PC a PC via Internet sem necessidade de licença. Normalmente são usados programas (gratuitos ou não) existentes no mercado que utilizam a Internet como meio de transmissão de voz.

Há tanto o VoIP puro como o híbrido, que mescla com saídas e entradas de outros sistemas. O VoIP puro é nada mais que a comunicação que se estabelece entre dois sistemas informáticos conectados à Internet, sem intermédio do PSTN. Há ainda o POTS, que é a comunicação que se estabelece entre um sistema PSTN e outro sistema de VoIP. E há um terceiro modelo de VoIP para

POTS onde o VoIP é utilizado para transportar “segmentos” da chamada telefônica com uso de PSTN, porém este não finaliza a ligação (Interconexão).

A convergência entre comunicação e computadores influencia sistemas regulatórios de maneira única, pois há diferenças intrínsecas no conjunto de regras de telecomunicações e sistemas de informação. Muitas dúvidas e controvérsias têm surgido a partir deste panorama vislumbrado com o surgimento de prestadores de VoIP. Principalmente, pela discussão se VoIP é serviço ou tecnologia³⁰⁷.

No aspecto legal, dependendo de como vai disponibilizar, se só para uso privado, ou entre matriz e filial, não precisa de autorização da ANATEL. Se for oferecer para terceiros, há a licença de SCM (Serviço de Comunicação Multimídia), que é para assinantes, privado, mas com interesse coletivo. Já o STFC (Serviço de Telefonia Fixa Comutada) é para todas as pessoas (ideia de universalidade). Ainda pode ser considerado Serviço de Valor Adicionado (caso de VoIP de computador para computador, por não ser considerado serviço de telecomunicação).

Logo, podem prestar serviços de VoIP as empresas que possuem licença do tipo SCM ou STFC. Entretanto, o serviço a ser prestado deve limitar-se às condições previstas em cada licença, ou seja, o STFC destina-se ao público em geral e o SCM deve ser prestado em regime privado. São licenças distintas para públicos diferentes. No entanto, este tema não é pacífico, pois há quem discuta até a necessidade de qualquer licença.

O SCM é um serviço fixo de telecomunicações de interesse coletivo, prestado em âmbito nacional e internacional, no regime privado, que possibilita a oferta de capacidade de transmissão, emissão e recepção de informações multimídia, utilizando quaisquer meios, a assinantes dentro de uma área de prestação de serviço. Uma empresa que possui essa licença pode prestar serviço privativo e não exclusivamente de voz. Esse serviço pode ser prestado, por exemplo, no âmbito de um Campus Universitário, ou dos órgãos de uma prefeitura ou ainda para Assinantes Corporativos.

A exploração de VoIP ou Telefonia IP, como serviço de interesse coletivo, é permitida via licença SCM. Entretanto, não é STFC, não é público, não obedece às regras de Numeração, Interconexão etc. do STFC e não tem, em consequência, direito às outorgas do STFC. Mas será que deve ficar sem regras?

307. Fontes para este capítulo: <<http://www.anatel.gov.br/>>, <<http://blog.ihcenter.com.br/?p=22>>, <<http://www.voipcenter.com.br>>.

Para o usuário residencial ter acesso à Telefonia IP ele deve ser assinante desse serviço junto aos prestadores de serviço habilitados de sua área. No Brasil esse serviço ainda não é oferecido aos usuários residenciais em regime local ou de longa distância nacional. Na longa distância internacional algumas operadoras já utilizam essa tecnologia, embora o usuário não tenha ciência desse fato quando faz esse tipo de chamada telefônica usando seu aparelho convencional.

No caso de uma empresa ter uma rede corporativa privada (virtual ou não) e pretender utilizar VoIP para a comunicação interna dentro da sua rede, em princípio, só é necessário uma licença no caso de a empresa ser um prestador de serviço de voz para terceiros. Para uso próprio não é necessário ter a licença.

Para uma empresa terminar tráfego internacional (STFC) de operadoras de Telefonia IP no Brasil é necessária a licença de STFC, na modalidade Longa Distância Internacional, considerado-se apenas o transporte do tráfego internacional. De outra forma, para terminar tráfego internacional de Voz de operadoras de Telefonia IP no Brasil, nenhuma licença é necessária, considerando-se apenas o transporte do tráfego de Telefonia IP via Operadora Internacional ou via PASI (Provedor de Acesso a Serviços Internet).

No entanto, se o VoIP é tão inevitável quanto eminente, devido ao seu baixo custo, vamos ponderar a respeito da capacidade atual de criptografia destes ambientes e suas principais vulnerabilidades, em especial no tocante à contaminação por vírus, *trojans*, furto de dados, interceptação e acesso indevido a sistemas, com possível repercussão em fraude eletrônica.

Logo a estrutura do mercado de VoIP exige a implementação de uma estratégia técnico-legal de arquitetura da informação ainda mais complexa, para garantir nível de serviço, qualidade, rentabilidade, privacidade e segurança da informação.

Final, é possível “grampo no VoIP”? Para muitos especialistas, sim³⁰⁸, bem como tudo o que está sendo transformado de voz em dados pode ser objeto de monitoramento e armazenamento. Por isso, o usuário desse tipo de

308. Lei n. 9.296/96 — “Art. 1º A interceptação de comunicações telefônicas de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta lei e dependerá de ordem do juiz competente da ação principal, sob sigilo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicação em sistemas de informática e telemática”.

serviço deve verificar se ele possui algum tipo de criptografia. Há modalidades gratuitas que não oferecem qualquer proteção³⁰⁹.

Para uso de VoIP a segurança depende do *software* de comunicação, pois o processo é voz, vira dados no computador e trafega na rede VoIP. Se não houver o padrão de *encryption* pelo fornecedor, a empresa e o usuário dificilmente poderão criptografar a mensagem previamente.

Outra questão a ser estudada envolve o limite que a tecnologia VoIP impõe para a Justiça, pois como fica um pedido de interceptação de comunicação telefônica no ambiente VoIP? E como atender ao direito já estabelecido para serviços de telefonia para o usuário acessar serviços emergenciais via telefone? Estas questões não estão respondidas nem regulamentadas. É um tema que deve permanecer sob o nosso estudo e acompanhamento.

8.45. Web 2.0 — redes sociais e seus impactos

Estamos vivendo a cultura das interfaces gráficas, conforme muitos autores já descreveram³¹⁰, em que o computador, de fato, transforma nossa maneira de criar e comunicar na era digital. Não apenas apelidos e avatares, mas verdadeiras redes sociais estão sendo construídas, onde pessoas se relacionam completamente de modo eletrônico, trabalham juntas, namoram, sem nunca se terem encontrado pessoalmente.

Chama-se isto de *wikinomics*, ou seja, o poder da colaboração em massa, como um novo modelo de infraestrutura típico de geração de conhecimento de baixo custo, em que pessoas e empresas colaboram de forma “aberta” para impulsionar a inovação.

309. Ex.: o Skype faz criptografia da voz transmitida, com o algoritmo AES — *Advanced Encryption Standard*, usando uma chave de 256 bits. A troca das chaves feitas no início da transmissão usa padrão de criptografia RSA. É compatível com o *Firewall* da empresa para uso da Porta TCP/IP 80, mas não funciona no caso da empresa barrar qualquer tráfego na porta 80 que não seja protocolo HTTP.

310. Recomendações bibliográficas: WEINBERGER, D. The hyperlinked metaphysics of the Web, <<http://www.hyperorg.com/misc/metaphysics/index.html>>. LÉVY, Pierre. *O que é o virtual?* São Paulo: Editora 34, 2001. RAYMOND, E. Catedral e o bazar, 1998 — Traduzido por Erik Kohler, <http://pt.wikisource.org/wiki/A_Catedral_e_o_Bazar>. COSTA, Rogério da. Por um novo conceito de comunidade: redes sociais, comunidades pessoais, inteligência coletiva, <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1414-32832005000200003&lng=pt&nrm=iso&tlng=pt>. RHEINGOLD, H. *Smart Mobs: The Next Social Revolution*. Perseus Books, 2003. MUSSO, Pierre. A filosofia da rede. In: *Tramas da rede*. Porto Alegre: Sulina, 2004. Org. André Parente. BARBROOK, R. Cibercomunismo: como os americanos estão superando o capitalismo no ciberespaço; Tradução: Barbara Nickel, <<http://members.fortunecity.com/cibercultura/vol4/cibercom.html>>.

Aquilo que nos diferenciava nos primórdios da civilização, em que os acidentes geográficos determinavam o isolamento de povos e cidades e provocavam inclusive o surgimento de variáveis do idioma, agora cede lugar para a acessibilidade total, sem fronteiras espaciais, em que se fala uma única linguagem, a das *Wikis*³¹¹.

A maioria das pessoas estava confinada a papéis econômicos limitados, seja como consumidores passivos de produtos produzidos em massa, seja como funcionários presos em burocracias organizacionais nas quais o chefe diz o que fazer. No entanto, o cenário atual vem romper com tudo isso, onde a tecnologia da informação permite que milhões de pessoas unam forças em colaborações auto-organizadas, que produzem novos bens e serviços dinâmicos e que rivalizam com os das maiores empresas. A isso hoje se define como *peer production*.

De certo modo, é como se o modelo de cooperativas tradicional tivesse ganho um irmão da era virtual. Mas o desafio é a capacidade de gestão desse modelo, em que se deve conseguir aplicar metodologias que preservem o padrão de qualidade. Esta é a maior crítica atual. Temos como exemplo, a *Wikipedia*, cujo conteúdo carece de qualidade e, muitas vezes, inclusive, está equivocado ou é falso. Muitas empresas já monitoram o que está dito sobre elas mesmas nestes ambientes, especialmente as abertas em bolsa, de modo a evitar que a informação inverídica venha a impactar o valor de suas ações.

Já faz parte da rotina de diversos profissionais usar sua rede de contatos eletrônica (do inglês *network*) para buscar respostas e soluções a seus problemas, participando de *sites* que reúnem pessoas, ou que fazem uso de conteúdos de terceiros (que não foi produzido pelo próprio *site*), sejam estes seus usuários ou localizados a partir de ferramentas dentro da Internet³¹².

Também já há diversas iniciativas em que a empresa cria um ambiente de colaboração interno, para funcionários, ou até mesmo externo, envolvendo fornecedores, parceiros e até clientes, para receber novas ideias e sugestões. No

311. Ver também artigo "Efeito-puxadinho" e transformação do mundo, o desafio do *open social*, de Hermani Dimantas e Dalton Martins.

312. Ex.: *mashup* é um *website* ou uma aplicação *web* que usa conteúdo de mais de uma fonte para criar um novo serviço completo. O conteúdo usado em *mashups* é tipicamente código de terceiros por meio de uma interface pública ou de uma API. Outros métodos de codificação de conteúdo para *mashups* incluem *Web feeds* (exemplo: RSS ou Atom), *Javascript* e *widgets* que podem ser entendidas como miniaaplicações *web*, disponíveis para serem incorporadas a outros *sites*, como: Google, Slide, Fotolog, Orkut, Youtube, Flickr e outros.

entanto, apesar de atraente, o uso de colaboração em massa e demais formatos de *Web 2.0*³¹³ exigem alguns cuidados jurídicos específicos.

Todos querem fazer parte da *Web 2.0*. As redes sociais se multiplicam. As marcas estudam formas de entrar nesta corrida pela interação com o internauta. Mas como participar de modo a agregar valor para a empresa e evitar riscos legais e institucionais, principalmente considerando que o controle está nas mãos do usuário?

Conteúdo, esta é a palavra-chave da Internet. Pelo menos da parte que experimentamos até aqui, a Internet neste primeiro momento apenas foi o receptáculo de toda a nossa produção cultural, todo o nosso conteúdo, por assim dizer.

A *Web 2.0* é um movimento que indica uma tendência pela quebra de alguns paradigmas, derivado da observação de características comuns aos serviços que se estão consolidando como os mais importantes da Internet.

No entanto, alguns aspectos jurídicos fundamentais devem ser observados: a questão autoral³¹⁴ e a questão trabalhista. Ou seja, se uma empresa convida para participar de suas atividades um funcionário terceirizado, ele pode depois alegar vínculo empregatício? Ou se envolver um cliente e a ideia deste for usada, o mesmo querer uma remuneração? Como a empresa pode se proteger desses riscos jurídicos? Mesmo a decisão de que o que for feito será de domínio público necessita da ciência e concordância de todos os envolvidos que participaram, e é formal, não tácita, senão corre-se o risco de eventualmente alguém ajuizar ação pleiteando direitos morais e patrimoniais sobre a obra.

A internet deixou de ser apenas uma rede de computadores e se consolidou como uma rede de pessoas; pessoas que participam cada vez mais, que querem se expor, seja por meio da divulgação de textos, comentários em *blogs*, compartilhamento de *links* ou apenas pela publicação das fotos de seu último aniversário.

A interatividade que movimenta o formato atual da *web* apresenta um panorama completamente novo, pois os produtores são, ao mesmo tempo, o

313. Segundo Hernani Dimantas, em seu artigo "As redes sociais — potência, subjetividade e o impacto Flaboração", dentro da análise da construção (ou reconstrução) do conceito de redes sociais, a Internet não está necessariamente ligada a computadores e sim às pessoas que o utilizam como ferramenta para a comunicação. Para ele, virtual é uma palavra mal compreendida. Virtual é tão real como o presencial.

314. Em princípio, em obras coletivas os direitos patrimoniais serão exercidos pelo organizador (inteligência do § 2º do art. 17 da Lei n. 9.610/98).

público e este também é composto por pessoas que estão apresentando ideias, divulgando materiais que outras pessoas fizeram ou colaborando com o aprimoramento de conteúdo já publicado.

Não podemos esquecer, entretanto, que na Internet as leis também são aplicadas. Por isso, é fundamental que quem participa dela, seja por meio de um *blog* muito visitado ou apenas por meio das redes sociais, conheça seus direitos e deveres, de forma a produzir com comprometimento.

A principal questão que tem chegado até nós diz respeito ao equilíbrio entre liberdade de expressão e os direitos de terceiros, tais como o direito à privacidade e à intimidade e também os direitos autorais. É indubitável que os direitos à expressão e à livre manifestação de pensamento são pilares democráticos que devem ser defendidos e preservados.

Quando o próprio internauta gera, manuseia, edita o conteúdo, tem que se ter todo o cuidado para que isso não promova a prática de ofensas digitais, em que os crimes contra a honra são os mais comuns (difamação, calúnia e injúria), bem como o uso não autorizado de imagem de pessoas, além da própria infração de direito autoral, com plágio de conteúdos sem menção de autoria. A principal recomendação é: deixar a informação clara antes da participação do usuário. Para tanto é preciso ter um termo de uso do ambiente colaborativo cujo texto deve tratar desses dois pontos detalhadamente. Esse documento tem relevância como prova legal do que ficou combinado entre as partes. Se for via *web*, tem de ser apresentado como barreira de navegação e devem ser guardados os *logs* referentes ao *click-ok* (ciência), associado a um cadastro. É muito importante que o ambiente não seja anônimo. Além disso, deve fazer menção da lei aplicável, especialmente quando envolve participantes de várias localidades e/ou países.

O cadastro é essencial para se saber a autoria, especialmente em caso de infração de direitos autorais de terceiros, que pode ocorrer em hipótese de alguém escrever um conteúdo (ideia, texto, foto, imagem, música, outros) que não é legitimamente seu e a empresa usar. Logo, o que perguntar no cadastro faz toda diferença para blindagem jurídica do ambiente. Deve-se ainda incluir algumas vacinas legais, tais como a declaração “a sua participação é voluntária, não onerosa, de modo algum há geração de qualquer vínculo empregatício ou remuneração”, assim como é importante ter canal de denúncia.

Além disso, é recomendável trabalhar o ambiente de modo diferenciado se nele houver a participação de menores de 16 anos. É claro que tudo o que é preenchido em cadastros na Internet tem característica declaratória, logo, se o usuário mentir, incorre nos crimes de falsidade ideológica, falsificação de documento, falsa identidade, entre outros. Mas para evitar responsabilidade soli-

dária do prestador do serviço, ou das Marcas associadas ao ambiente interativo, é essencial que o texto deixe isso claro.

Não há como dar a devida proteção jurídica sem definir o que se quer com o ambiente colaborativo. Ou seja, o que será feito com o conteúdo por ele produzido e inclusive de quem será a responsabilidade. Se o ambiente ficar em uma intranet, sem exposição pública na Internet, há menos riscos, mas se for para ficar com o máximo de visibilidade, pode ser importante ter um responsável editorial para retirar comentários ofensivos ou declarações não condizentes com os objetivos institucionais do ambiente ou da empresa que o promove. A forma de fazer faz toda a diferença para não ter risco legal.

Sempre que um conteúdo for postado, a fonte deve ser citada e um conteúdo alheio não deve ser apresentado como próprio. A lei brasileira protege o autor, e a reprodução de uma obra deve ser devidamente autorizada; se quiser, o usuário pode postar pequenos trechos e direcionar seu leitor, por meio de *links*, por exemplo, ao conteúdo completo e original, mas nunca publicar o texto integral que foi feito e divulgado por outrem.

Logo, em termos legais, o modelo de negócios da geração de conhecimento colaborativo deve levar em consideração alguns pontos fundamentais. A responsabilidade pelo conteúdo publicado é uma delas. Talvez a mais relevante. Afinal, se há uma pessoa ou empresa como entidade centralizadora ou organizadora, ela será responsável ou corresponsável, como se fosse um condomínio de conhecimento.

Sendo assim, quando uma empresa implementa um modelo de *wiki*, envolvendo funcionários, parceiros, clientes, é essencial que haja um Termo de Participação Colaborativa que deixe claras estas questões, tanto de quem é a responsabilidade, quais os limites da participação, como de quem é a propriedade do que for gerado e como será feita ou não a distribuição da riqueza e os créditos de autoria.

Se o modelo permitir anonimato, o seu risco legal será aumentado. Desta forma, em âmbito corporativo, deve-se ter um processo de autenticação da entrada do colaborador, com guarda dos *logs* de ciência ao termo, bem como exigência de apresentação de dados válidos de identidade.

Estamos passando por uma profunda transformação do modelo socioeconômico produtivo, das próprias relações de trabalho, e a Justiça ainda tem como visão e leis o modelo anterior. Por isso, são os contratos, os termos de uso, os *disclaimers*, avisos legais nas interfaces que determinam as regras que as partes convencionaram que evitam riscos legais. Se não se falar nada, corre-se o risco de que a produção colaborativa dê uma boa dor de cabeça e prejuízo ao final.

Alguns podem alegar que ideal é a liberdade total, a falta justamente de regras. Bem, pode até funcionar, mas se em algum momento alguém se indispuer com outro e a situação parar na justiça, vai fazer falta não ter criado a regra do jogo e não ter passado ela no próprio jogo, de forma clara, objetiva, entre os participantes. Na era da informação, é a própria informação que garante a proteção legal.

O modelo do Youtube é reflexo de nossa sociedade atual. O mundo virtual deve ser regido por regras de conduta ética. Há liberdade de expressão, mas há limites também. E estes estão baseados nas leis vigentes. As marcas que querem associar-se a esta nova Internet, que acreditamos que não é um modismo ou uma tendência, veio para ficar, e, para evoluir para ambientes de mobilidade, precisam estar atentas para promover o uso ético e legal destes espaços e não serem coniventes, nem correrem o risco de ser responsabilizadas pela prática de ilícitos e crimes.

A melhor estratégia jurídica se passa por usar a linguagem do meio, em se colocar as vacinas legais nas próprias interfaces gráficas, assim como se fosse um grande jogo *online*. Não se deve reprimir, mas sim orientar. Não se pode omitir, é essencial informar. E assim vamos evoluir para uma dinâmica social real-virtual saudável e construtiva, geradora desta nova riqueza, de ativos intangíveis, de conhecimento.

Mais recentemente assistimos ao fenômeno do *Twitter*. Um dos seus grandes diferenciais foi abrir para participação corporativa, em que empresas podem passar a ter um perfil. Virou verbo — *twittar*. Mas que tipo de informação as pessoas e as empresas brasileiras publicam no *Twitter*? Há dois tipos de abordagens: há empresas que possuem presença direta, assumida, como um canal oficial, postando as mesmas informações que poderiam ser encontradas no *site* e há uma segunda estratégia que é agir por meio de um interlocutor, por exemplo, o diretor de RI, de Comunicação, de SAC, em que publica comentários e opiniões sobre a empresa, o tom é mais de ordem pessoal, se colocando a disposição para interagir com os demais, tirar dúvidas e indicar o acesso do *site* da empresa para complemento das informações. Há uma intenção de ir até o potencial investidor onde ele está, mas deve-se ter muito cuidado para não ficar forçado, pedante, e assim a comunicação gerar uma reação negativa.

Interessante lembrar que, embora o uso das redes sociais seja majoritariamente focado no compartilhamento de informações pessoais, os consumidores estão no mundo digital e suas vozes têm ganhado força junto às empresas, que não querem acumular máculas em sua reputação digital.

Mas, assim como pessoas físicas, as marcas também têm direito à preservação de sua reputação, de acordo com entendimento de juristas e tribunais

brasileiros. Sendo assim, recomendamos que o direito à reclamação seja exercido sem abusos, sem promoção, por exemplo, de alterações em nomes e logomarcas de marcas registradas.

Há de se falar, hoje em dia, na herança digital; e o que isso significa? Por mais que as pessoas participem das redes sociais, documentam tudo o que fazem com publicações, fotografias, vídeos etc., elas algum dia virão a falecer e deixar todo o conteúdo publicado na *web*. Existem serviços que gerenciam a rede social da pessoa, armazenando a senha do usuário ou, até mesmo, redes sociais que podem excluir o perfil ou transformá-lo em um memorial, sendo administrado pela família. Para que este último aconteça, será necessário que a família comprove (com a certidão de óbito) que a pessoa faleceu.

Ainda estamos aprendendo, concomitantemente às mudanças constantes do cotidiano *online*, a lidar com as questões jurídicas que surgem diariamente com a *web* interativa. A própria lei brasileira de direitos autorais está em questionamento e já conta com anteprojeto para que seja alterada.

As empresas devem estar atentas quando fizerem uso de ambientes de redes sociais para não gerarem confusão junto ao público-alvo da empresa, sejam investidores, colaboradores, clientes, isto é, a informação deve ser consistente, quer seja com uma abordagem corporativa quer com uma mais pessoal. Afinal, é uma informação por escrito que compromete sempre a empresa. Deve-se evitar “achismos”, deve-se evitar “informações desconstruídas” e “informações não oficiais”. Dicas e recomendações mais direcionadas a determinados públicos é um bom complemento, pois em um ambiente de rede social pode-se assumir um “tom” mais relacionado com determinado público-alvo. Por exemplo, a empresa quer atrair um estudante universitário ou quer atrair um investidor estrangeiro. Ela poderá utilizar linguagens distintas para cada um, até mesmo imagens, cores, mas o conteúdo tem de ser o mesmo no sentido mais financeiro (não pode haver previsões distintas de crescimento, mas pode-se enfocar temáticas diferentes para gerar mais interatividade).

Até mesmo a Administração Pública observou a necessidade em participar mais de redes sociais para interagir com os cidadãos, mesmo que seus perfis em redes sociais sejam apenas informativos. Temos como exemplo a Secretaria de Gestão Pública do Estado de São Paulo, que publicou a Resolução SGP n. 15, de 25 de junho de 2009, que prevê a revisão de critérios e a criação de regras de acessibilidade para possibilitar o acesso dos servidores públicos à Internet, bem como às ferramentas sociais e Web 2.0.

Toda mídia tem seus riscos, no caso destes ambientes, o principal risco está relacionado à exposição em si, à própria interatividade. Se a empresa atua com

consumidor final, em um mercado que é comum ter bastante contencioso judicial, ela deve estar preparada para encontrar reações negativas a sua presença em redes sociais, bem como para saber lidar com os ambientes mais ofensivos, que extrapolam os limites da liberdade de expressão e do direito de reclamação do consumidor (entra no abuso de direito previsto no art. 187 do Código Civil). Deve-se preparar bem os cenários e os discursos, pois havendo uma situação assim, de incidente de imagem e risco reputacional, deve-se agir rapidamente, não há tempo para ficar fazendo reuniões de alta direção, pois a coisa se espalha rápido, inclusive os boatos eletrônicos. Logo, ter um plano de ação que preveja não só o que a empresa quer falar, mas o que ela não quer falar, e o que ela terá de falar se alguém falar algo contrário a ela.

Além disso, a empresa deve estar preparada para o fato de que é possível alguém criar um perfil falso no nome da empresa ou de algum executivo da mesma. Já tivemos casos no escritório que resolvemos rapidamente no início do *Twitter*, mas assim como outros ambientes de redes sociais, já não estão mais atendendo a solicitação de exclusão do perfil falso via notificação extrajudicial rapidamente. E o *Twitter* não tem representação legal no Brasil, o que faz com que uma medida legal deva ser ajuizada nos EUA (São Francisco) diretamente para ser mais eficaz, pois ajuizar no Brasil pode levar 12 meses só para distribuir a solicitação de citação para Justiça Americana (carta rogatória).

A empresa deve refletir sobre o quanto a Internet pode impactar a opinião de seus *stakeholders*. Nesse sentido é melhor estar nela do que estar fora dela. É melhor estar presente e combater informação com informação. Pois é muito comum quem está em uma rede social não ir até o *site* da empresa, inclusive, pode-se usar a presença em um *Twitter* para ensinar este hábito, de se encontrar a informação no *site* da empresa.

A empresa deve selecionar bem quem cuidará deste ambiente e monitorá-lo permanentemente. Deve ser alguém com legitimidade para falar em nome da empresa como seu porta-voz, até porque será sempre bem difícil afastar a responsabilidade da empresa sobre o conteúdo (algo como foi o fulano, não foi a empresa), a não ser na hipótese de perfil falso. Não importa o cargo, deve ser alguém bem preparado para lidar com situações que ocorram de momento com os demais participantes.

Destacamos que é importante a empresa gerar uma norma interna e divulgar a todos os seus colaboradores sobre a postura dos mesmos na Internet e em redes sociais, lembrá-los do compromisso com sigilo profissional, da proteção de fato relevante etc. Pois acontece muito de os funcionários acabarem tendo também presença nestes ambientes e publicarem conteúdos contraditó-

rios ao que a empresa está dizendo. Tivemos um caso em que a empresa discursava sobre governança verde (meio ambiente) e havia uma comunidade de um colaborador que publicou uma pesquisa feita pela área dele que apontava não conformidades com itens ambientais. Outro caso envolveu um Vice-Presidente com uma postura oposta (no perfil do Orkut que ele tinha) ao que a empresa prega no mercado. É comum a empresa decidir sobre a sua participação oficial nestes canais e esquecer de orientar todos os seus colaboradores, terceiros e parceiros sobre a participação deles que possa impactar a imagem da empresa.

A construção de uma cultura de companhia aberta é um dever de casa permanente, até pelo *turn over* de pessoas. E muitos entendem que devem consultar a área de RP ou Marketing para falar com a imprensa oficial, mas não para falar ele mesmo em seu *blog*, comunidade, fórum da Internet. E isso pode significar que a empresa é aberta em bolsa, que um comentário em uma rede social, publicado por um colaborador, terceirizado ou mesmo por alguém da alta direção, não percebendo que risco ou consequência possa ser gerado, vir a infringir a Instrução n. 348 da CVM, por ser declaração de fato relevante.

Atualmente, em muitas empresas, não fica clara a diretriz, qual a postura esperada, institucionalizada em uma política interna, em um Código de Conduta que deve por certo ser atualizado com todas essas novas ferramentas de comunicação que surgiram. A reputação digital de uma empresa, de uma marca, atualmente, também se passa pela reputação digital de seus dirigentes, por certo, e os riscos de segurança da informação se passam pela prática digital de todos os seus colaboradores.

Estando ou não a empresa nas redes sociais, ela deve preparar-se para as manifestações digitais, que ocorrem independentemente de sua vontade. Logo, monitorar a Internet é essencial, é dever de casa de RI, como do Marketing, do RH, do SAC, da área de Segurança da Informação, cada um com seu objetivo de monitoração. Tanto é que hoje prestamos um serviço de monitoração legal do ambiente para vários clientes, onde fazemos varreduras periódicas, identificamos os incidentes, diagnosticamos e orientamos a empresa, é um serviço de inteligência jurídica, pois muitas vezes a solução se passa por uma estratégia de comunicação e não uma medida judicial. Mas deve-se medir sempre os riscos jurídicos envolvidos.

É um ônus da empresa monitorar o que se passa na *web*, pois como não há censura prévia (não há como evitar tudo isso), o importante é ser o primeiro a saber e agir rápido. Novamente, às vezes, a demora (fator tempo) é mais prejudicial do que o conteúdo em si. A empresa deve criar normas internas claras, treinar (orientar e educar na cultura de companhia aberta na era do

conhecimento, das informações geradas por todos e não mais só pela empresa) e monitorar permanentemente.

Portanto, seguem as principais recomendações para blindagem legal das empresas nas redes sociais:

- Realizar um planejamento estratégico antes de ingressar nas redes sociais é fundamental. Identifique para qual propósito a sua empresa pretende utilizar este novo canal. Por exemplo: atendimento ao cliente, promoções, notícias, sugestões, entre outras;

- Elabore um guia de conduta para seus colaboradores apoiarem de forma segura, ética e legal a presença da sua empresa nesse canal e um Manual de Uso da marca nos canais eletrônicos;

- Tenha um plano de resposta a incidentes definido. Você deve estar preparado para situações do gênero;

- Transparência. Sempre apresente as informações da maneira mais clara possível;

- Cuidado com a publicação de informações confidenciais, divulgação de boatos ou assuntos pessoais nestes canais corporativos. As informações são disseminadas de modo muito rápido e estão relacionadas à sua empresa;

- Realizar treinamentos de capacitação com a equipe responsável pela administração das contas;

- Não deixe de responder as mensagens enviadas. O perfil deste usuário/consumidor é imediatista;

- Varie o conteúdo publicado. Esteja aberto a elogios e críticas. Desenvolva e mantenha sempre atualizado um procedimento para atuar em cada uma destas situações, principalmente em crises;

- Monitoramento. Acompanhe sempre o que os usuários estão falando de você;

- Utilize as redes sociais de acordo os Termos e Condições estabelecidos por elas. Cada canal possui regras próprias para utilização e constantemente são atualizadas.

O passo mais importante para a proteção da empresa no tocante às redes sociais é a conscientização de suas equipes, não apenas colaboradores, mas inclusive os terceirizados e parceiros, pois basta um comentário para gerar um grande risco reputacional, financeiro e jurídico. Logo, seguem algumas dicas que têm sido utilizadas em campanhas educativas internas. Mesmo que a empresa não libere o acesso às mídias sociais a partir de uma conexão à internet corporativa, a maioria dos colaboradores participa das mesmas, a partir

de seus dispositivos particulares, em especial *smartphones* ou *tablets*, durante o horário de expediente, então, precisa-se orientar:

- Não associe conteúdo pessoal ou de opinião particular com a marca da empresa em que trabalha;

- Não divulgue informações da sua rotina de trabalho;

- Não publique informações classificadas como interna ou confidencial;

- Não ofenda outros colaboradores, clientes, parceiros ou fornecedores, nem tampouco manifeste sua opinião nestes perfis corporativos;

- Tenha uma postura ética, segura e dentro das leis nas redes sociais. Dependendo do cargo que ocupar, qualquer manifestação, mesmo que pessoal, pode gerar impacto na sua empresa;

- Evite o excesso de exposição;

- Em hipótese alguma, gere contato ou publique informações que possam configurar concorrência desleal (p. ex.: contatar equipe de concorrente pedindo informações ou oferecendo vaga de trabalho);

- Respeite os Direitos Autorais. Sempre cite a fonte ou a referência do conteúdo publicado;

- Utilize fotos ou imagens previamente autorizadas pelas pessoas nelas retratadas;

- Na dúvida sobre o que pode ser publicado em rede social, peça autorização antes.

Que venham os *twitters*, *flickr*s, *wikis*, os *youtubes*, os *second lifes*, os *third lifes*, e tantos outros. Quem quer ganhar com a *Web 2.0* deve estar preparado para entregar mais do que mero conteúdo aos seus Clientes. Assim como deve verificar sempre o que estará associado a sua marca, e, sempre que possível, participar na orientação de valores para formação de usuários digitalmente corretos, como sendo um requisito inclusive de responsabilidade social digital.

8.46. Monitoramento da Marca na Internet

Uma coisa é a discussão de monitoramento de pessoas, mas como fica o monitoramento de marcas? É interessante pensar que uma pessoa jurídica é um fenômeno de ficção do Direito, já que, na verdade, de forma simplificada, o conceito de empresa consiste na reunião de pessoas com um objetivo social em comum (objeto social). Logo, pode uma empresa receber a proteção jurídica de sua “imagem e reputação”? Existe dano moral à empresa? Em nosso entendimento, sim.

Desse modo, o que vem a ser a Marca Digital? Seria o resultado da experiência que se dá em qualquer momento de contato com a marca nos ambientes eletrônicos, com todos os seus diversos públicos (*stakeholders*). Consiste no conjunto das Relações da Marca, por meio de tudo o que permita manifestação de vontade, expressão, informação e comunicação!

Logo, a Sociedade Digital trouxe várias vantagens para a consolidação das marcas. Mas toda essa facilidade também ajuda para que nomes respeitados ou que ainda estão disputando uma posição no mercado sejam facilmente copiados e atacados.

Quanto melhor a reputação da marca, mais suscetível ela se torna a golpes virtuais. É muito comum seu uso indevido, incluindo o *marketing* paralelo, falsificação da marca e seus produtos, enfraquecendo seriamente a confiança dos clientes, danificam o valor da sua marca, podendo até mesmo colocar em risco os seus consumidores.

Diante deste novo cenário de oportunidades, mas também de riscos, faz-se essencial o monitoramento permanente da Marca na Internet, para identificação rápida e quase imediata de situações de incidentes em andamento ou na eminência de ocorrer.

Ambientes como Orkut, Wikipédia, Youtube, *blogs*, entre outros, são ricos em manifestações positivas e negativas em nome da Marca. Além disso, aproveitando a grande procura e necessidade por nomes de domínio, fraudadores criaram o *CyberSquatting* e *TypoSquatting*, técnica que consiste em registrar domínios com termos e marcas famosas ou com uma grafia semelhante. Essa tática desvia usuários distraídos para páginas com conteúdo adulto, ilegal, *sites* de concorrentes, gerando um *marketing* negativo, bem como podendo gerar riscos legais. Mas a lei pune este tipo de conduta, tanto no Brasil como internacionalmente³¹⁵.

315. Legislação para proteção de marcas e domínios contra ação de fraudadores e oportunistas:

- Internet Corporation for Assigned Names and Numbers — ICANN;
- Constituição Federal, art. 5º, XXIX;
- Lei n. 9.279/96 — Propriedade Industrial;
- PL n. 256, de 2003 — Requisitos para o registro de nomes de domínio no Brasil;
- Resolução 002/2005, revogada pela Resolução 008/2008, da CGI.br;
- Federal Trademark Ailution Act (FTDA);
- Anticybersquatting Consumer Protection Act (ACPA).

Logo, também ocorre concorrência desleal na Internet, especialmente na forma de uso indevido de sinal distintivo alheio. A solução jurídica para este tipo de problema envolve primeiramente o envio de uma notificação extrajudicial, para dar ciência ao fato, contando um prazo “a partir de”. Uma vez que não há procedimento administrativo para impugnar o registro junto ao “www.registro.br”, nem previsão específica na legislação brasileira, só existem duas formas possíveis de procedimento, autocomposição ou processo junto à Justiça Estadual.

Quando identificado este tipo de incidente, deve-se rapidamente coletar a Ata Notarial, após enviar a notificação extrajudicial, e se as tratativas amigáveis falharem, ajuizar ação no Judiciário ou dar entrada em um pedido de arbitragem internacional.

Considerando a relevância do fator “tempo” para o exercício do próprio Direito Digital, é sempre bom tentar evitar o processo judicial clássico, não pela discussão de mérito, já que se a Marca é legítima e registrada com prova de anterioridade, é muito difícil perder a causa, mas sim pela demora. Para tentar contornar isso, é possível pedir a tutela antecipada, uma vez que é normal nestes casos o magistrado deferir o congelamento do *site* até a conclusão da lide, no entanto, são raros os casos em que a Justiça tenha deferido a transferência antecipada.

Uma outra situação que é comumente identificada pelo monitoramento é o uso de “marca registrada” como palavra-chave em *link* patrocinado³¹⁶. Neste caso, há prática de concorrência desleal por “uso de artifício fraudulento para desvio de clientela”³¹⁷.

Outro caso também recorrente é a identificação de texto incorreto ou inapropriado inserido na *Wikipedia* no nome da Marca. A *Wikipedia* é considerada a maior enciclopédia *online*, grande fonte de pesquisa, não apenas para estudantes, jovens, mas inclusive para a imprensa. A enciclopédia é baseada na

316. Nomenclatura de modelo de publicidade *online* ofertada em alguns serviços de busca na Internet, como o Google.

317. Práticas fraudulentas contra ativos intelectuais em geral configuram crime de concorrência desleal, previstos em lei. Para ocorrer concorrência desleal, além da atividade fraudulenta, é necessário que:

- Agentes econômicos produzam ao mesmo tempo;
- No mesmo espaço geográfico;
- No mesmo segmento mercadológico;
- Ou seja, que eles concorram de fato.

produção colaborativa de conteúdo, de maneira simples e rápida, promovendo a democratização da informação e do conhecimento; contudo, é necessário observar a veracidade das informações constantes nos textos do *site*, e, dependendo do caso, fazer uma solicitação de retificação.

Finalmente, um ponto que merece destaque diz respeito à criação de comunidades, seja de clientes ou funcionários; a lei é clara no tocante à proteção de marcas e patentes. Há comunidades de consumidores, funcionários, ex-funcionários, parceiros, entre outras. Para verificar os riscos jurídicos envolvidos na exposição da Marca Digital, as comunidades precisam ser analisadas sob quatro aspectos de gestão de risco: a) Segurança da Informação; b) Consumidor/Relacionamento; c) uso de Marca não autorizado; e d) Quebra de Sigilo Profissional³¹⁸.

Não quer dizer que sempre há o que ser feito juridicamente. Muitas soluções são muito mais institucionais do que jurídicas. Mas é requisito para um gestor olhar o que está se passando com a marca na Internet e, a partir do monitoramento e do diagnóstico, decidir qual a melhor medida a tomar. Isso pode fazer toda a diferença inclusive para avaliação do valor de marca, em situações de Fusões e Aquisições e outros tipos de *valuation*.

8.47. E-Política — aspectos legais das eleições na Internet

Não se pode mais ignorar o fenômeno das eleições *online*. Primeiro, porque este ambiente já se provou como excelente plataforma de informações positivas ou negativas sobre candidatos, partidos e governos. Quer seja o seu uso para construção de imagem, ou para guerrilha eleitoral, a Internet tem-se consolidado, não apenas no Brasil, mas também em outros países, como canal influenciador em tempo real, com toda a possibilidade da multimídia e sem tempo de duração. Isso quer dizer que não se esgota no tempo do programa partidário obrigatório. Há quem diga que é uma ferramenta essencial para o próprio exercício transparente e democrático das eleições.

Um grande fator motivador do uso da Internet também é o seu custo baixo. Isto é, sai mais barato o *e-mail marketing* do que o “santinho”. É possível gerar métricas, saber quantas pessoas estão clicando em uma palavra-chave de

318. Tratam desta matéria ainda os arts. 186 e 927 do Código Civil, art. 325 do Código Penal, art. 482, alínea *b, g, h e j* da Consolidação das Leis do Trabalho, Lei n. 9.279/96, Lei n. 8.112/90, inciso VIII do art. 116 e Lei n. 7.170/83, em seu art. 13.

um buscador para saber mais sobre um candidato, um partido, ou sobre temas, como trabalho, saúde, educação, segurança pública. Todavia qual o limite de uso desta mídia? Deve ser regida como as demais?

O uso de *sites, blogs, comunidades, chats, messenger, e-mail marketing*, entre outros, permite que haja eleições não apenas a cada dois anos, mas todo o tempo e de modo interativo. Isso pode ser muito bom por um lado; mas, se não houver um certo controle, pode acabar se tornando invasiva.

Claro que em ano de eleição, especialmente presidencial, a disputa fica acirrada e não se pode estar fora da Internet. Não ter informação *online* é uma desvantagem para o candidato. Até porque se combate a informação com mais informação e não com omissão. Mas há regras que precisam ser seguidas. É neste sentido que o TSE tem regulamentado as eleições e tratado do tema de Internet nos últimos anos. A propaganda política no Brasil é disciplinada em Lei e, a cada pleito, o TSE baixa uma Resolução específica³¹⁹ que regulamenta a disputa eleitoral, além, é claro, da aplicação das regras já estabelecidas no Código Eleitoral, na Lei n. 4.737/65 e na Lei n. 9.504/97. O ano de 2010 é um marco neste tema por causa da mudança da Lei Eleitoral, que passou a admitir amplamente o uso da Internet PLC n. 141/2009 (PL n. 5.498/2009 no Senado Federal).

A primeira das normas que regulamentou o uso da Internet em campanhas eleitorais no Brasil foi a Lei n. 9.504, de 30 de setembro de 1997. À época não existia ainda sequer um entendimento de que poderia existir de alguma maneira a propaganda política na Internet, de forma tal que os dispositivos do texto legal tratam apenas de estender as vedações impostas às emissoras de rádio e televisão aos sítios que as mesmas porventura viessem a manter na Internet.

Diante da inexistência de legislação específica para a propaganda eleitoral na Internet, o Tribunal Superior Eleitoral (TSE), desde as eleições municipais do ano de 2000, regulamentou, para *sites* de candidatos, o uso do domínio “*www.nome_do_candidato_número_do_candidato.can.br*”, como forma de organizar a propaganda na Internet. Nesse sentido, o TSE elaborou uma *home page* orientando sobre o registro desse domínio especial³²⁰.

319. Para as eleições de 2008 é a Resolução n. 22.718; já para as eleições de 2006 aplicou-se a Resolução n. 22.158; nas eleições de 2004 foi a Resolução n. 21.610; nas eleições de 2002 aplicou-se a Resolução n. 20.988, de 5-2-2004, do Tribunal Superior Eleitoral, e assim por diante.

320. “*Tanto é que, para propiciar o equilíbrio entre candidatos, abriu-se a possibilidade da pá-*

Nas eleições de 2002 ficou definido que o candidato que quisesse publicar sua *home page* na Internet deveria providenciar seu registro com a nomenclatura <http://www.nomedocandidatonumerodocandidatouf.can.br>, sendo proibida qualquer propaganda eleitoral por meio de páginas de provedores de serviços de acesso à Internet, em qualquer período.

No entanto, muito se questionou sobre a obrigatoriedade do uso do domínio específico para o candidato, principalmente com o crescimento de redes sociais e a necessidade de ir até onde está o eleitor e não ter que ele fazer vir até onde está o candidato. Há que se considerar que existem vários tipos de *home pages* — página do candidato, página da campanha, página do partido, página institucional de Ente Público, *Blog* de Campanha, Orkut de Campanha, perfil em outras redes sociais, como o Twitter e o Facebook.

Se um usuário clica em uma palavra-chave e chega ao *site* com informações do candidato, isso não deveria ser propaganda, a não ser que o candidato esteja pedindo votos, que esteja comentando já sobre as eleições ou fazendo qualquer referência a ela ou colocando o número da legenda³²¹.

Além disso, deve ser observado o prazo de proibição de campanha eleitoral nas 48 horas que antecedem as eleições e até 24 horas após, sob pena de configurar boca de urna eletrônica³²². Este tipo de situação é muito difícil de se evitar que ocorra.

gina de propaganda registrada no órgão gestor da Internet Brasil, com a terminação 'can.br', nos termos do art. 78 da Res. - TSE n. 21.610/2004, com despesas a cargo do candidato, cujo domínio será cancelado após o primeiro turno, ressalvado aos candidatos concorrentes em segundo turno. 2. Seria indubitavelmente inócua a solução encontrada pela Justiça Eleitoral, relativamente ao domínio 'can.br' — o qual, evidentemente, não poderia ser obrigatório —, se fosse ele desprezado, para que o candidato viesse a se utilizar de tantos outros 'sites' que pudesse custear, para veiculação de sua campanha, em prejuízo dos menos aquinboados financeiramente. 3. Recurso desprovido" (Ac. n. 24.608, de 10-2-2005, rel. Min. Caputo Bastos).

321. Acordo Gabeira x TRE/RJ — Pré-candidato não retira *site* do ar e levanta discussão sobre liberdade de acesso à Internet. Um dos argumentos de Gabeira a favor da liberdade na Internet é o de que ninguém é obrigado a acessar nenhum *site*. Segundo ele, as pessoas procuram na Internet aquilo que lhes interessa, assim como um leitor compra na banca o jornal de sua preferência. “*Se entram na minha página é porque querem saber de mim. Eu não tenho como controlar também o que falam de mim no Orkut, é humanamente impossível. (...) Vou lutar dentro dos limites legais. Não podemos ter no Brasil a mesma visão que os chineses tem da Internet. Vou estudar como posso entrar na Justiça para poder pedir a anulação desse item na legislação eleitoral.* Cumprindo um acordo verbal com o TRE do Rio, não mencionado na matéria do *Jornal do Brasil*, a entrevista publicada no *Le Monde Diplomatique* será retirada, até que tenhamos uma reunião sobre o tema. Depois disto, vou começar a batalha legal pela liberdade na internet. Batalha que, na verdade, envolve a todos, inclusive a liberdade dos adversários”. Fonte <<http://www.gabeira.com.br/blog/#>>>.

322. Código Eleitoral, art. 240, parágrafo único.

No tocante a jurisprudências do TSE, cabe ressaltar que as questões que envolvem a propaganda eleitoral na Internet já são objeto de disputa desde as eleições do ano de 2000. Contudo, o posicionamento do Tribunal Superior variou bastante desde a análise dos primeiros casos até a data presente, e deve ainda mudar mais nas próximas, conforme o amadurecimento do próprio tema³²³.

Sendo assim, no assunto de eleições, a Internet é inevitável. Esta é a grande certeza para as eleições no Brasil. Ela aumenta o acesso à informação para um público de eleitores que está cada vez mais conectado, como os jovens eleitores na faixa dos 16 anos. Isso será feito por meio das redes sociais, por

323. Mais Jurisprudências:

“Propaganda eleitoral. Internet. Antevéspera do segundo turno. Autorização. 1. É razoável a manutenção das páginas institucionais das candidaturas à Presidência da República no mesmo período da propaganda regular por rádio e televisão, no caso, durante o dia 27 de outubro. 2. Pedido deferido” (Res. n. 22.460, de 26-10-2006, rel. Min. Carlos Alberto Menezes Direito).

“Representação. Propaganda eleitoral mediante *site* da Internet não autorizado pela Justiça Eleitoral. Procedência em parte” (Ac. de 26-10-2006 na Rp 1.301, rel. Min. Ari Pargendler).

“Representação. Programa eleitoral gratuito. Proibição. Decisão. Representação anterior. Veiculação. Conteúdo. Internet. Ausência. Prova. Responsabilidade. Representados. Ônus. Representante. (...) 1. A comprovação da responsabilidade dos representados pela veiculação de propaganda na Internet, já proibida por decisão em anterior representação, constitui ônus do representante. (...)” NE: Veiculação, em *sítio da Internet, de vídeo de programa proibido em representação anterior* (Ac. de 25-9-2006 no AgRgRp 1.131, rel. Min. Marcelo Ribeiro).

“Representação. Divulgação. Candidatura. Internet. Ausência. Conhecimento. Beneficiário. Propaganda eleitoral. Extemporaneidade. Violação. Art. 36 da Lei n. 9.504/97. Art. 72 da Res.-TSE n. 21.610/2004. Materialidade. Autoria. Comprovação. Multa. Aplicação. Representação julgada procedente” (Ac. de 21-3-2006 na Rp 788, rel. Min. Caputo Bastos).

“Recurso especial. Representação. Propaganda eleitoral. Veiculação. *Banners. Sites*. Internet. Natureza. Comercial. Período. Vedação. Legislação eleitoral. Circunstância. Amplitude. Acesso. Interessado. Notícia. Circulação. Procedência. Aplicação. Multa. Motivo. Comprovação. Desequilíbrio. Igualdade. Oportunidade. Candidato. Participação. Eleição. Faculdade. Utilização. Propaganda. Página. Registro. Órgão. Gestor. Internet Brasil. 1. A discussão de que o proibitivo de propaganda se refere a páginas de provedores, ou a tratadas no § 3º do art. 45 da Lei n. 9.504/97, permitindo-a em sites pessoais, não é mais absoluta ante a jurisprudência recente.

“Presença de candidato em ‘sala de bate-papo’ mantida por provedor de acesso à Internet, para responder perguntas de ‘internautas’. Hipótese que não caracteriza propaganda eleitoral e, por isso, impede a aplicação da sanção prevista no art. 36, § 3º, da Lei n. 9.504, de 1997” (Ac. 2.715, de 26-4-2001, rel. Min. Sálvio de Figueiredo, red. designado Min. Fernando Neves).

“(…) Propaganda eleitoral irregular. *Site* da Internet. Responsabilidade. Não há previsão legal para a imposição de multa a candidato, com base no art. 45 da Lei n. 9.504/97, que é dirigido tão somente às emissoras de rádio e televisão e às empresas de comunicação social que mantêm sítios na Internet. (...)” (Ac. 16.004, de 7-10-1999, rel. Min. Maurício Corrêa).

“Homepage da Radiobrás na Internet contendo informações sobre a Presidência da República. Caráter informativo. Propaganda eleitoral não configurada. Recurso improvido” (Ac. 140, de 8-10-1998, rel. Min. Luiz Carlos Madeira).

e-mail, por meio de um *site*, um *blog*, debates em *chats* ou vídeos postados no YouTube, fotos e textos espalhados por toda a *web*.

A grande questão, agora, não é mais se deve haver eleições na Internet, mas como deve ser feito. Regulamentar a forma de uso é o melhor meio de evitar abusos e deixar claras as regras para quem participar da disputa. A Internet vai acontecer, movida inclusive pelos próprios eleitores, que falarão de seus candidatos nos ambientes virtuais.

Mas como está a legislação do Brasil para o uso da Internet? Com o que ocorreu nas eleições dos EUA, e o grande *case* apresentado por Sam Graham-Felsen, o “garoto” de 28 anos, responsável por eleger Barack Obama, todos querem saber como fica o assunto para as próximas eleições presidenciais no Brasil. Por que é tão polêmica a discussão sobre este tema, que divide opiniões inclusive no próprio Tribunal Superior Eleitoral? No Brasil existem dois grupos de regras para a propaganda eleitoral: *a*) um conjunto fixo, composto pelo Código Eleitoral e pela Lei n. 9.504/97, que é válido para todas as eleições realizadas em solo nacional; e *b*) um conjunto variável, composto pelas Instruções do TSE (Tribunal Superior Eleitoral), que mudam bastante e geralmente são válidas apenas para uma eleição específica.

Como o conjunto fixo não tem disposições sobre a Internet de modo mais detalhado, a regulamentação no Brasil das questões *online* em eleições costuma variar a cada pleito. Nas eleições municipais de 2008, o TSE emitiu a Instrução n. 121, dispondo que “a propaganda eleitoral na Internet somente será permitida na página do candidato destinada exclusivamente à campanha eleitoral” e que “os candidatos poderão manter página na Internet com a terminação .can.br, ou com outras terminações, como mecanismo de propaganda eleitoral até a antevéspera da eleição” (arts. 18 e 19). Ou seja, os candidatos e partidos só podiam fazer propaganda em *site* próprio e específico para isso. Propaganda em Orkut ou YouTube, por exemplo, seria analisada caso a caso (o que levou, por exemplo, a Justiça paulista a intimar a organização da campanha de Geraldo Alckmim a retirar todos os vídeos de publicidade do candidato do Youtube).

Isso nos leva a compreender o sentido da propaganda eleitoral antecipada, que é a venda da imagem de determinado candidato como o mais apto ao exercício da função pública antes do período eleitoral. Dessa forma, é possível manter *sites* (institucional, *blog* etc.) e perfis em redes sociais (Twitter, Facebook, YouTube etc.) fora do período eleitoral, mas é preciso estar atento que a imagem do possível candidato não esteja sendo vendida, como já foi visto em diversas jurisprudências³²⁴.

324. Jurisprudências:

Durante as eleições de 2008, diversos candidatos se insurgiram contra o TSE por não concordarem com essa instrução. Mas o tribunal não acatou seus pedidos, alegando que o período eleitoral já havia começado e seria impossível mudar as regras da publicidade para a eleição em curso.

Este foi o motivo do alvoroço em torno do Projeto de Lei n. 5.498/2009, sancionado pelo Presidente Luiz Inácio Lula da Silva, em 30 de setembro de 2009, sob a Lei n. 12.034/2009, que libera o uso da Internet para eleições, mas sem as restrições já em vigor para debates realizados em TV e rádio. No entanto, não poderá haver propaganda política paga na *web*, pela redação que ficou aprovada. É fundamental, também, manter a distinção do que é “ato de vontade” daquilo que é “propaganda eleitoral”. Um candidato ter sua informação na *web* disponível para o eleitor por meio de uma ferramenta de busca e navegação é perfeitamente válido, legítimo e legal.

“Representação. Propaganda antecipada. Divulgação. Texto. Internet. *Blog* Conotação Eleitoral. Presente. Recurso. Desprovemento. (...) 2. O fato de o acesso a eventual mensagem contida em *sítio* da internet depender de ato de vontade do internauta não elide a possibilidade de caracterização da propaganda eleitoral extemporânea, caso nela conste “pedido de votos, menção ao número do candidato ou ao de seu partido ou qualquer outra referência à eleição” (...) 4. Divulgada, por meio de página na internet, a candidatura e os motivos pelos quais a candidata seria a mais apta para o exercício do cargo público, é de se reconhecer a prática de propaganda antecipada” (TSE, Recurso em Representação n. 203.745, rel. Min. Marcelo Henriques Oliveira, publ. em 12-4-2011).

“Recurso eleitoral. Propaganda eleitoral antecipada. Eleições 2010. Comunidade no Orkut. Mensagens. Pré-candidatura. Divulgação. Conteúdo eleitoral. Caracterização. Direito à livre manifestação do pensamento. Violação. Inexistência. Aplicação do § 3º, art. 36, da Lei 9.504/97 (...) 3. A criação de comunidade no ambiente virtual do Orkut, contendo mensagem com nítida alusão a cargo eletivo pretendido, ao momento das eleições, bem como à conduta de pré-candidata, caracteriza propaganda eleitoral antecipada, ainda que não haja pedido expresso de voto ou divulgação do número da legenda partidária. Recurso improvido” (TSE, Recurso Especial Eleitoral 96.326, rel. Min. Arnaldo Versiani Leite Soares, publ. em 2-3-2011).

“Eleições 2010. Propaganda Eleitoral. Twitter. Direito de resposta. *Sítios* de mensagens instantâneas e assemelhados. Possibilidade jurídica. 1. O Twitter se insere no conceito de ‘*sítios* de mensagens instantâneas e assemelhados’, previsto no art. 57-B da Lei 9.504/97, e é alcançado pela referência a ‘qualquer veículo de comunicação social’ contida no art. 58 da Lei das Eleições. 2. O direito de resposta em razão de mensagem postada no Twitter é cabível. Relevância de o detentor da página ser coordenador de comunicação de campanha eleitoral. 3. Deferido o direito de resposta, o próprio usuário, exercendo o controle de conteúdo que detém sobre a sua página no Twitter, deve postar o texto da resposta. 4. Direito de resposta concedido” (TSE, Representação 361.895, rel. Min. Henrique Neves da Silva, publ. em 29-10-2010).

“Responsabilidade civil. Candidato a vice-prefeito que é ofendido em fórum de discussão de *site* de relacionamentos Orkut. Manifestações que ultrapassam o regular exercício da liberdade de expressão. Ultraje à honra e imagem atributo do autor, que há anos foi vereador da cidade. Sentença parcialmente reformada, apenas para reduzir a indenização para R\$ 7.500,00. Recurso provido em parte” (TJSP, Apelação 994.09.299693-0, rel. Des. Enio Zúliani, j. 12-8-2010).

Com a mudança da Lei Eleitoral³²⁵, chega ao fim a exigência de uso exclusivo do domínio “.can.br”, mas os candidatos têm de registrar seus *sites* oficiais no TSE. Ficou definido que a propaganda eleitoral gratuita será permitida em *blogs*, *sites*, comunidades e outros veículos de comunicação do próprio candidato, além de portais de notícias. Eleitores que quiserem fazer *sites* de apoio a políticos estão livres.

325. Nova Lei Eleitoral em vigor no Brasil — alteração da Lei n. 9.540/2007

Situação	Como era até 2010	Como é a partir de 2010
DOAÇÃO A CANDIDATO E PARTIDO	Pessoa física ou jurídica (exceto as que tenham função pública — art. 31 da Lei n. 9.504/97) — pode fazer doações de valores a candidatos (art. 39 da Lei n. 9.504/97). MEIOS DE DOAÇÃO: cheque cruzado e depósito bancário em conta do partido (art. 39 da Lei n. 9.096/95).	Pessoas físicas passam a fazer doações via <i>web</i> , por meio dos <i>sites</i> dos partidos e candidatos além da doação de valores por meio de cartão de crédito (altera o art. 23 da Lei n. 9.504/97).
DEBATES NA WEB	Atualmente, emissoras de rádio ou televisão podem promover debates, desde que respeitadas as seguintes regras: I — nas eleições majoritárias (candidato é eleito pelo maior número de votos. Ex.: eleição para Presidente da República), a apresentação dos debates poderá ser feita: (i) em conjunto, estando presentes todos os candidatos a um mesmo cargo eletivo; e (ii) em grupos, estando presentes, no mínimo, três candidatos; II — nas eleições proporcionais (candidato é eleito por um percentual de votos. Ex.: eleição para deputados). Os debates deverão ser organizados de modo que assegurem a presença de número equivalente de candidatos de todos os partidos e coligações a um mesmo cargo eletivo, podendo desdobrar-se em mais de um dia.	Os debates poderão ser realizados na Internet sem aplicação das regras impostas ao rádio e TV. As regras impostas aos debates a ser veiculados em rádios e TV foram alteradas: (i) deverão ser acertadas entre a pessoa jurídica que irá veiculá-los e os partidos políticos, dando-se ciência à Justiça Eleitoral. As regras aplicáveis aos debates feitos no 1º turno das eleições devem ser estipuladas com a concordância de 2/3 de candidatos de partidos com representação na Câmara dos Deputados — no caso de eleição majoritária — e de 2/3 dos partidos ou coligações com candidatos aptos — em caso de eleição proporcional (insere os §§ 4º e 5º, no art. 46 da Lei n. 9.504/97).
CENSURA PRÉVIA	A Justiça Eleitoral, a requerimento do candidato, pode censurar previamente propaganda quando concernente à apresentação de propaganda ofensiva à honra de candidato, moral ou bons costumes (art. 53, § 2º, da Lei n. 9.504/97).	Dispõe que o poder de polícia se restringe às providências necessárias para inibir as práticas ilegais, vedada a censura prévia sobre o teor dos programas a ser exibidos na televisão, no rádio ou na Internet (altera o § 2º do art. 41 da Lei n. 9.096/95).
DIREITO DE RESPOSTA	Prevê o exercício do direito de resposta em veículos de comunicação social, regulamentando o seu exercício em órgãos da imprensa escrita, programação normal de rádio e TV e em horário eleitoral gratuito (art. 58 da Lei n. 9.504/97).	Inclui a possibilidade de exercício do direito de resposta na <i>web</i> , regulamentando-o. Acrescenta que tramitarão com prioridade na Justiça Eleitoral as representações para exercício do direito de resposta pretendidas em qualquer meio de comunicação (inclui o inciso IV, no art. 58 da Lei n. 9.504/97).

Para os que quiserem utilizar a Internet ou outros espaços de publicação de opiniões próprios, é fundamental evitar situações de dano a imagem e reputação. A melhor prática é gerar a oportunidade do direito de resposta, também previsto na lei aprovada, como forma de se manter isento. Devem-se monitorar comentários, retirar do ar os que forem abusivos (após ciência, não previamente, pois seria censura), e conferir o direito de resposta à parte vítima.

PROPAGANDA ELEITORAL ANTECIPADA	Não enumera nenhuma situação, tanto de propaganda eleitoral antecipada ou que não a configure. Decisão caso a caso pela Justiça Eleitoral.	Enumera situações que não poderão ser consideradas como propaganda eleitoral antecipada, tais como: participação de filiados a partidos políticos ou pré-candidatos em entrevistas, programas, encontros ou debates no rádio, TV e na Internet; realização de encontros e seminários a expensas do partido político em ambiente fechado etc., desde que não haja pedido de votos, observado pelas emissoras de rádio e TV o dever de conferir tratamento isonômico (inclui o art. 36-A na Lei n. 9.504/97).
PROPAGANDA ELEITORAL NA INTERNET	É possível a propaganda eleitoral na Internet desde que feita no <i>site</i> do candidato ou do partido político (art. 18 da Resolução n. 22.718/2008).	Mantém a redação do <i>caput</i> da emenda do Senado: assegura a liberdade de manifestação de pensamento na Internet e em outros meios eletrônicos de comunicação interpessoal, garantindo o direito de resposta em casos de ofensa e vedado o anonimato. <i>Sites</i> de veículos jornalísticos também poderão publicar textos opinativos sobre os candidatos (altera o art. 57-D da Lei n. 9.504/97).
MENSAGENS ELETRÔNICAS	Proibidas atualmente (Resolução n. 22.832/2008, que regulamentou as eleições de 2008).	Permitidas (inclui o art. 57-B, III na Lei n. 9.504/97). As mensagens devem ter <i>opt-out</i> , e canceladas em 48h, sob pena de multa de R\$ 100,00 por mensagem indevidamente enviada (inclui o art. 57-H na Lei n. 9.504/97).
PROPAGANDA PAGA NA INTERNET	Proibidas atualmente (Resolução n. 22.832/2008, que regulamentou as eleições de 2008).	Rejeita a emenda do Senado e veda a veiculação de propaganda paga na Internet. É proibida a propaganda paga na Internet (inclui o art. 57-C na Lei n. 9.504/97).
VEICULAÇÃO, NO ANÚNCIO, DO VALOR PAGO PELA PROPAGANDA	Nada dispõe sobre a obrigatoriedade de veiculação do valor do anúncio, no próprio veículo de propaganda.	Dispõe que deverá constar do anúncio, de forma visível, o valor pago pela sua inserção, nas propagandas feitas em jornal impresso e reproduzidas na Internet (inclui o § 1º ao art. 43 da Lei n. 9.504/97).
VEDAÇÃO DE PROPAGANDA NA INTERNET	Proibida a propaganda eleitoral na <i>web</i> atualmente (Resolução n. 22.832/2008, que regulamentou as eleições de 2008).	É vedada apenas em <i>sites</i> : oficiais ou de órgãos ou entidades da administração pública direta ou indireta; de pessoas jurídicas com ou sem fins lucrativos e com destinação profissional (inclui o art. 57-C, § 1º, I, II e III na Lei n. 9.504/97).
CADASTROS ELETRÔNICOS	Nada dispõe sobre o tema.	Veda a venda de cadastros de endereços eletrônicos a partidos, candidatos ou coligações (insere o art. 57-E na Lei n. 9.504/97).

Ainda não poderemos usar a Internet para propaganda política paga, mas já houve alguns avanços, inclusive na possibilidade de doação *online*, bem como fazer *e-mail* marketing com a inclusão da opção *opt-out*. O que se tem de grande aprendizado é que não se pode regulamentar a Internet usando analogias. Não há motivo para restrição da *web* como ocorre com TV e rádio, até porque não há 30 milhões de eleitores *online* na mesma página, e a comunicação não é interruptiva da navegação do usuário. Isso compromete a natureza deste meio, vocacionado pela liberdade de expressão. No entanto, deve-se coibir o anonimato, o que também foi previsto e aprovado no projeto. Mas será difícil evitar a boca de urna digital.

Devemos destacar que o uso das redes sociais amplia a capacidade de mobilização na campanha eleitoral. A Internet como mídia gera um diferencial de aproximar o candidato dos eleitores, diretamente, além de alcançar um público eleitor mais jovem, o que pode fazer toda diferença nas próximas eleições presidenciais, que é o que ocorreu na campanha do Barack Obama.

Para o Brasil, o uso da Internet nas eleições vai permitir maior informação e diálogo sobre os candidatos, os partidos, as propostas e, inclusive, vai atrair o público que já não acompanha mais este tipo de discussão em outras mídias tradicionais, com propaganda obrigatória como TV e rádio. A Internet é ine-

PENALIDADES AOS PROVEDORES QUE DESCUMPRIREM A LEI ELEITORAL	Nada dispõe sobre o tema.	As penalidades da Lei Eleitoral somente serão aplicadas aos provedores quando houver comprovação de prévio conhecimento da veiculação de propaganda irregular ou envolvimento na divulgação do conteúdo, bem como se o provedor intimado a retirar propaganda irregular não tomar as providências no prazo determinado para tal (altera a redação do art. 57-F, proposto pela Câmara no PL n. 5.498/2009, e acolhe parcialmente a emenda do Senado).
DOCUMENTO COM FOTOGRAFIA PARA VOTAÇÃO	Nada dispõe sobre o tema, sendo permitida a votação sem apresentação de documento com fotografia.	Impõe ao eleitor que apresente seu título de eleitor na hora da votação e um documento com foto (inclui o art. 91-A na Lei n. 9.504/97).
VOTO IMPRESSO NAS ELEIÇÕES DE 2014	Nada dispõe sobre o tema.	Altera a Lei n. 9.504/97 e determina que, a partir das eleições de 2014, 2% das urnas eletrônicas deverão imprimir o comprovante de votação (art. 5º do PL n. 5.498/2009).
PERMANÊNCIA DA PROPAGANDA NA WEB	Nada dispõe sobre o tema, mas com relação às outras modalidades de propaganda veda, desde 48h antes até 24h depois da eleição, propaganda política mediante radiodifusão, televisão, comícios ou reuniões públicas (parágrafo único do art. 240 da Lei n. 4.737/65).	Não há limite temporal para a veiculação de propaganda eleitoral gratuita na Internet, considerando-se que, aos demais veículos de comunicação, a propaganda eleitoral deve ser suspensa 48h antes do dia da votação e 24h depois. Assim, a propaganda eleitoral pode permanecer na <i>web</i> inclusive no dia da votação, sem qualquer suspensão.

vitável para uma realidade de sociedade do conhecimento, e pode trazer também mais transparência. O desafio é o controle dos abusos. Há necessidade de se coibir as ofensas, que podem ocorrer em razão do grande anonimato que a rede permite e que é vedado pela Constituição Federal, como já dissemos, para que possa haver o uso saudável da Internet nas eleições. É preciso educação e não censura.

Acredito que a maturidade se conquista com a experiência, com o uso da rede. Quanto mais for usada, melhor ficaremos no tocante ao seu uso responsável, já que o mau uso será denunciado e devidamente punido pelo Tribunal Superior Eleitoral. Como já vem acontecendo desde 2004, em situações que já envolvem diversos candidatos e a Internet. A grande diferença é que agora as redes sociais se tornaram um espaço de grande disputa, de maior atenção e interesse devido ao seu poder de mobilização, e não mais apenas ter um *site* do candidato ou participar de algum debate em *chat*. A tendência é que seja criada uma espécie de "Código de Conduta do Candidato na *web*", respeitando a privacidade dos eleitores e os demais candidatos. Será um grande desafio conseguir controlar "o *spam* eleitoral", com toda certeza.

Muitas agências já têm experiência em marketing digital, em ações virais, no uso de ambientes de redes sociais, mas em uso estratégico da Internet nas eleições, de forma séria e relevante na campanha, não.

Nas eleições de 2010, tornou-se possível a arrecadação de valores para campanhas eleitorais via Internet, já que a alteração da Lei n. 9.504/97 inseriu o inciso III do § 4º do art. 23, permitindo que somente as pessoas físicas fizessem doações por meio da Internet pelo *site* do partido ou do candidato, inclusive por cartão de crédito, durante a data das eleições. A arrecadação *online* também exige melhores práticas, durante a prestação de contas da campanha eleitoral de candidatos, comitês financeiros e partidos. Dentro das prestações de contas é preciso descrever de forma bem clara as doações que foram feitas durante o período eleitoral; todas as doações recebidas mediante o uso de cartão de crédito serão lançadas individualmente. Importante ressaltar que cada doação possui um limite de valor (art. 23, § 1º, I) e que, caso ultrapasse, e o candidato não tiver conhecimento, isto é, não souber a procedência do valor doado, isso não ensejará responsabilidades deste nem a rejeição de suas contas eleitorais. Por óbvio isso foi feito para evitar possíveis fraudes e enriquecimento ilícito por campanhas eleitorais.

Estamos gerando um momento propício para que isso ocorra, e é muito importante que tais agências estejam bem assessoradas no tocante aos limites jurídicos, ao uso ético, seguro e legal, para evitar riscos para o candidato e o partido, bem como punições.

A melhor forma de fazer uso de redes sociais nas eleições é tomar proveito da espontaneidade, ou seja, o responsável pela campanha do Obama, Sam Graham-Felsen, disse que eles criaram um ambiente, que se multiplicou, espontaneamente, inclusive gerou mais de 13 milhões de *e-mails* cadastrados na base de dados. Deve-se evitar condutas muito agressivas e ofensivas, inclusive no sentido de ridicularizar os outros que estão na disputa. O uso da produção mais multimídia, de fazer filmes para circularem nestes ambientes também dá muito resultado, mas precisa usar a linguagem da rede, o que é um grande erro é pegar o que se fez padrão da campanha para as mídias tradicionais e jogar na *web*, não dá certo. Tem de ser feito sob medida para *web*, já que a Internet não permite analogias.

A Internet oferece muito mais transparência às eleições. Acirrará a disputa nos *mouses* e celulares de toda uma nova geração de cidadãos digitais. Os estrategistas políticos precisarão criar peças específicas para Internet, como foi feito na campanha do Obama, não se pode usar esta mídia como se fosse comunicação de massa. Este será um grande desafio. Ao final, esperamos que nas próximas eleições possam mostrar que somos usuários digitalmente corretos e sabemos extrair o melhor que este meio pode proporcionar.

8.48. Espionagem eletrônica

Para iniciar o estudo sobre espionagem eletrônica, é essencial analisar o cenário no qual a Sociedade Digital está inserida. Com o crescente uso de tecnologia por pessoas e empresas, o que faz com que fiquemos cada vez mais conectados, a possibilidade de ocorrência de espionagem pela via eletrônica também cresce³²⁶, facilitada ainda pela falta de prevenção e proteção, já que não há um hábito de segurança da informação estabelecido em nível cultural.

Logo, a cada dia que passa, aumenta o número de empresas vítimas de espionagem eletrônica no mundo³²⁷ e também no Brasil. De certo modo, vive-

326. Relatório do FBI — <http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf> este é do próprio FBI e relatório do Computer Security Institute — <<http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>>.

327. Isso ocorreu com a consultoria Booz Allen Hamilton, em que um executivo recebeu um *e-mail* cujo conteúdo tratava da descrição de aviões, motores e equipamentos para radar, mas o mesmo continha um código conhecido como “Poison Ivy” (espécie de cavalo de troia) destinado a capturar os dados. Logo, no momento que o executivo selecionasse as imagens para ver, o mesmo seria baixado e instalado no computador, e a partir de então passaria a espionar tudo que ele fizesse no computador. Fonte: <http://www.businessweek.com/magazine/content/08_16/b4080032218430.htm>.

mos uma realidade mais monitorada, e mais espionada. Além disso, há uma sutil diferença entre o limite do que é considerado “inteligência competitiva” e onde começa a prática de espionagem³²⁸ nas empresas.

Há vários tipos de espionagem eletrônica, entre elas, a mais comum é chamada de *Sigint*³²⁹ (*signals intelligence*) que se originou na interceptação, decodificação, tradução e análise de mensagens por uma terceira parte além do emissor e do destinatário pretendido.

Normalmente, a vulnerabilidade é interna³³⁰. Ou seja, no início, nos anos

328. Notícia: IT WEB datada de 15-7-2008 — Atul Malhotra, que foi vice-presidente de serviços de imagem e impressão da HP foi condenado por roubo de segredos comerciais da IBM. Seu julgamento ocorrerá em outubro, e ele pode pegar dez anos de prisão, multa de US\$ 250 mil e três anos de liberdade assistida. Entre 1997 e 2006, Malhotra, de 42 anos, trabalhou na IBM como diretor de desenvolvimento de negócios e vendas em Santa Barbara (EUA). Um mês antes de sair da companhia, ele pediu e recebeu um documento chamado CC (*Calibration Metrics*), um arquivo de preços marcado como confidencial. E foi advertido por um coordenador da área de preços a não redistribuir a informação. Em maio de 2006, Malhotra começou a trabalhar na HP, como vice-presidente de serviços de imagem e impressão. Em julho, ele enviou o documento confidencial da IBM, por *e-mail*, a colegas da HP. Os documentos que tramitam na justiça norte-americana não especificam como os *e-mails* de Malhorta foram detectados. O que se sabe é que ele usou o assunto “Apenas para você ver — confidencial” no campo assunto das mensagens.

329. Formas de Coleta de Informações, segundo Marco A. C. Cepik, autor da “Espionagem e democracia”:

- Humint (*human intelligence*) — “...o acrônimo em inglês que designa essa disciplina é um eufemismo tipicamente norte-americano, incorporado ao jargão internacional porque evita o uso do termo *espão*...”
- Sigint (*signals intelligence*) — “...originou-se de interceptação, decodificação, tradução e análise de mensagens por uma terceira parte além do emissor e do destinatário pretendido...”
- Imint (*imagery intelligence*) — “...posterior ao uso da aviação militar para reconhecimento e vigilância, durante e após as duas guerras mundiais do século XX. (...) Desenvolvimento de ‘imint’ como uma disciplina especializada de coleta de informações deu-se fundamentalmente a partir da associação entre o uso de câmeras fotográficas e plataformas aeroespaciais.”
- Masint (*measurement and signature intelligence*) — “No contexto norte-americano, faz parte da área de ‘masint’ desde a coleta e o processamento técnico de imagens hiperspectrais e multiespectrais até a interceptação de sinais de telemetria de mísseis estrangeiros... Passando pelo monitoramento de fenômenos geofísicos, pela medição dos níveis de radiação nuclear...”
- Osint (*open sources intelligence*) — “...consiste na obtenção legal de documentos oficiais sem restrições de segurança, da observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países...”

330. Conhecida como “risco *insider*”. O “espão interno” é considerado um “agente infiltrado”. Na história, há vários casos famosos:

— Juan Pujol Garbo: forneceu informações erradas ao exército alemão o que possibilitou o desembarque na Normandia (dia D). Foi até condecorado pelos nazistas pelos seus “feitos”. Sua identidade ficou desconhecida por mais de 40 anos.

— Dussan Dusko Popov: iugoslavo trabalhou para os ingleses na 2ª Guerra Mundial.

70 e 80, quando se falava de espionagem eletrônica sempre se estava referindo a um “ataque hacker”, a uma invasão. Mas isso mudou. A fragilidade está nas pessoas, principalmente no funcionário, seja ele próprio ou de empresa fornecedora (terceirizado), por diversos tipos de motivação³³¹, é envolvido para permitir o acesso ao ambiente (deixar a porta aberta), ou ele mesmo agir em nome de quem o contratou (pode ser coletando e enviando informações, pode ser apagando as mesmas na rede, entre outras situações). Há ainda o “laranja”, que seria aquela pessoa envolvida na espionagem por ingenuidade, inocência, ou até mesmo negligência.

Não há um crime específico de “espionagem eletrônica”; na verdade a conduta está tipificada em alguns artigos³³² do Código Penal brasileiro e da Lei

Descobriu com detalhes o plano de ataque aos americanos. Repassou diversas informações falsas aos alemães (prática de desinformação). O personagem James Bond é inspirado nele.

— *Eli Cohen*: forneceu informações fundamentais para vitória de Israel na Guerra dos 6 dias. Conseguiu se infiltrar no mais alto escalão do governo da Síria. Quase foi convidado para ser ministro da Defesa e foi o 3º na lista de sucessão para presidência da própria Síria.

— *Robert Hanssen*: agente do FBI, Hanssen invadiu o computador de Ray Mislock, oficial sênior de contrainteligência. Vendeu para a KGB (atual FSB) a identidade de agentes secretos alocados no leste europeu e comprometeu diversas operações.

— *Aldrich Hazen Ames*: foi preso pelo FBI em Arlington, Virginia, sobre acusações de espionagem em 24 de fevereiro de 1994. No momento da sua detenção, Ames era um veterano de 31 anos de Agência Central de Inteligência (CIA), espionava para os russos desde 1985. Ele foi preso com sua esposa, Rosario Ames, cúmplice de suas atividades de espionagem.

331. Motivação (motivo para ação), segundo Ira Winkler em *Spies Among Us*

- Dinheiro — motivo mais óbvio;
- Ideologia — algumas pessoas se sentem compelidas a se colocar em risco por uma causa (vide fanáticos religiosos);
- Chantagem (extorsão) — uso de informações do passado pessoais ou não que possam constranger ou coagir indivíduo a realizar ação indesejada;
- Ego — o simples fato de se achar mais esperto, merece mais que os demais colegas ou ainda por vingança. Fator puramente psicológico.

332. Dependendo do caso, deve-se analisar completamente o *modus operandi* para o correto enquadramento da conduta, que pode configurar o crime de concorrência desleal, o crime de violação de direito autoral, o crime de violação de segredo profissional, o crime de falsa identidade, o crime de dano, o crime de furto, o crime contra o sistema financeiro, entre outros:

— Art. 195 da Lei n. 9.279/96 — crime de concorrência desleal — “Comete crime de concorrência desleal quem: (...)”

III — *emprega meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem;* (...)

IX — *dá ou promete dinheiro ou outra utilidade a empregado de concorrente, para que o empregado, faltando ao dever do emprego, lhe proporcione vantagem;* (...)

XI — *divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam*

de Propriedade Industrial n. 9.279/96 (Marcas e Patentes) e pode envolver também as ações (forma de execução) que foram utilizadas para atingir o êxito. Devido a isso, inclusive, é muito difícil punir a tentativa de espionagem. No entanto, quando a empresa toma conhecimento, pode no mínimo rescindir o contrato de trabalho, quer seja por previsão do art. 482³³³ da Consolidação das Leis do Trabalho, seja por cláusula de contrato de prestação de serviços regida pelo Código Civil.

Mas como se proteger da espionagem? Com a facilidade de uso das ferramentas de trabalho tecnológicas, as informações da empresa vazam por todos os lados, desde o uso do *e-mail* até o uso da porta USB do computador (com dispositivos como *pen drive*, aparelho MP3, Câmeras fotográficas, entre outros). De funcionários mal treinados a mal intencionados que fornecem informações,

de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

XII — *divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude;*

Pena — detenção, de 3 (três) meses a 1 (um) ano, ou multa”.

— Art. 154 do Código Penal — crime de violação segredo profissional — “Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena — detenção, de três meses a um ano, ou multa”.

— Art. 184 do Código Penal — crime de violação direito autoral — “Violar direitos de autor e os que lhe são conexos: pena de detenção, de três meses a um ano, ou multa”.

333. Art. 482 da Consolidação das Leis do Trabalho: “Constituem justa causa para rescisão do contrato de trabalho pelo empregador:

- a) ato de improbidade;
- b) incontinência de conduta ou mau procedimento;
- c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço;
- d) condenação criminal do empregado, passada em julgado, caso não tenha havido suspensão da execução da pena;
- e) desídia no desempenho das respectivas funções;
- f) embriaguez habitual ou em serviço;
- g) violação de segredo da empresa;
- h) ato de indisciplina ou de insubordinação;
- i) abandono de emprego;
- j) ato lesivo da honra ou da boa fama praticado no serviço contra qualquer pessoa, ou ofensas físicas nas mesmas condições, salvo em caso de legítima defesa, própria ou de outrem;
- k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem;
- l) prática constante de jogos de azar”.

bem como fornecedores e terceirizados que possuem livre acesso e não estão nem orientados nem comprometidos contratualmente com segurança da informação são os ingredientes necessários para o incidente.

No dia a dia corporativo é comum altos executivos necessitarem de equipes de apoio, de secretárias a assistentes, e, muitas vezes, compartilhar sua senha com eles. Logo, quanto mais se sobe no nível hierárquico, maior o cuidado que se deve ter com segurança da informação, mas, ao mesmo tempo, maior probabilidade de as regras não serem cumpridas por quem está no topo da pirâmide.

Por que a secretária tem que ter a senha do chefe? Como garantir governança corporativa em uma empresa em que haja segregação de funções, ou seja, mais de uma pessoa é necessária para executar uma atividade de alto risco e impacto crítico no negócio, de modo que sozinho não deveria conseguir fazer um grande estrago na empresa. Mas o que normalmente acontece é um saber a senha do outro colega, dentro de um combinado para fazer o trabalho fluir mais rápido. Isso é completamente indevido, inadequado e quebra regras de conduta exigidas inclusive na assinatura de Códigos de Ética de conformidade com a Sarbanes-Oxley.

Além disso, é preciso vigiar os terceirizados, já que eles possuem livre acesso a vários tipos de informação, além de na área de TI serem responsáveis, em muitos casos, em dar suporte aos usuários (tipo *Help Desk*). Ou seja, é boa prática ter um Código de Conduta do Terceirizado com assinatura de termo de responsabilidade do funcionário terceirizado e a empresa contratada com a entrega de uma via para a empresa contratante.

Mas por que as ameaças internas são piores que as externas? Primeiramente, devido a maior chance de sucesso associado a menor chance de ser apanhado. Além disso, é muito mais fácil desenvolver uma ferramenta e mecanismos de vigilância para identificar uma invasão do que conseguir perceber uma conduta suspeita de um usuário legítimo. Ou seja, sem o devido preparo do terreno, praticamente os casos de espionagem só são pegos por denúncia e, mesmo assim, muitas vezes, nada se pode fazer devido à falta de provas ou sua origem ilícita.

Destaque-se, por oportuno, que a prova em um caso de espionagem é fundamental. Sem prova não há nada a fazer; logo a questão da perícia digital, do uso de computação forense, torna-se crítica para o deslinde da situação. Em muitos casos, apesar de se saber quem foi, não se pode punir a pessoa, pois as provas não foram coletadas da forma adequada, ou seja, não houve preservação do ambiente, ou não houve registro dos *logs*, ou estes foram registrados mas logo em seguida apagados, não houve solicitação de evidências para as teste-

munhas-máquinas de terceiros (provedores, outros) rapidamente, não houve perícia técnico-jurídica com uso de computação forense no computador, caixa postal de *e-mail*, entre outros.

Logo, os principais atributos de vantagem de um *insider* consistem no fato de normalmente seu acesso ser legítimo (tem a senha da rede); ele consegue praticar melhor engenharia social normalmente persuadindo outros colegas, manipulando a ingenuidade, inocência ou até mesmo a negligência das pessoas ao seu redor.

Para se proteger é essencial alinhar uma estratégia que amarra aspectos técnicos e jurídicos, com uso de alguns *softwares* de monitoramento³³⁴, com a devida adequação legal para que ele possa ser feito sem riscos para a empresa. Além disso, é essencial a definição de alguns processos e sua documentação em norma própria, alinhando com as melhores práticas de mercado³³⁵ e, acima de tudo, conscientização dos usuários de maior acesso a informações privilegiadas, dos gestores ao conselho.

Logo, para combater espionagem é essencial aplicar medidas em três níveis: físico, lógico e comportamental³³⁶, considerando:

334. De acordo com Celso Hummel, gerente regional da TechBiz Forense Digital, maior companhia brasileira de reação ao cibercrime e especializada no combate ao avanço das ameaças virtuais e na resposta a incidentes de segurança, "*avanços tecnológicos sem os devidos cuidados facilitam a ação dos fraudadores. Uma empresa bem protegida e capaz de reagir adequadamente aos crimes digitais pode diminuir perdas e recuperar receita em números expressivos caso seja vítima de espionagem industrial*". Fonte: <<http://www.techbiz.com.br>>.

335. ABNT NBR ISO/IEC 27001:2006 que trata dos procedimentos e recomendações sobre Sistemas de Gestão de Segurança da Informação e ABNT NBR ISO/IEC 21002:2005 (antiga 17999) que estabelece um Código de Prática para Gestão da Segurança da Informação.

336. É um equívoco acreditar que a segurança está garantida mediante um único controle. Conforme a "Teoria das Barreiras", a segurança é garantida pelo conjunto de medidas, e não apenas uma isolada:

— Barreira 1 — Desencorajar — é a barreira mais comum e consiste em fazer uso de câmeras de vídeo, avisos de segurança e alarme. Esta é a primeira das barreiras de segurança e cumpre papel importante de desencorajar as ameaças.

— Barreira 2 — Dificultar — dispositivos de autenticação de acesso físico com roletas, detectores, *firewall*. O objetivo desta barreira é complementar a anterior através da adoção efetiva dos controles que irá dificultar o acesso indevido.

— Barreira 3 — Discriminar — definir perfis e permissões. Aqui o importante é se cercar de recursos que permitam identificar e gerir acessos, definindo perfis e autorizando permissões.

— Barreira 4 — Detectar — monitoramento e auditoria, detecção de intrusão. Mais uma vez agindo de forma complementar às suas antecessoras, esta barreira deve munir a solução de segurança de dispositivos que sinalizem, alertem e instrumentem os gestores de segurança na detecção de situações de risco.

— Barreira 5 — Deter — bloqueio de acesso lógico ou físico. Esta quinta barreira representa o objetivo de impedir que a ameaça atinja os ativos que suportam o negócio.

a) criação de controles mais rígidos na área de Recursos Humanos, pois a maioria dos *insiders* possui um histórico de violação a políticas corporativas e/ou prática de crimes, mas há também informações sobre atividades extratrabalho, como família e mesmo em Orkut e *Blog* da pessoa que revelam muitas vezes o que está acontecendo;

b) fazer segregação de função, mas rever com frequência os acessos e, se possível, amarrar não apenas o *login* do usuário com uma senha, mas também a uma identidade de máquina;

c) criação de equipes com atividades específicas, a fim de que determinada tarefa que envolva confidencialidade ou risco não fique atrelada a somente um indivíduo, e sim a um grupo, a fim de cada um exerça uma fiscalização sobre o outro;

d) uso de *softwares* de monitoramento eletrônico, pois vigiar é essencial;

e) desenvolvimento e aplicação de Políticas de Segurança da Informação;

f) regulamentação do uso de dispositivos móveis, com bloqueio de portas USB, por exemplo, restrições de uso de determinadas mídias;

g) execução de ações de conscientização que englobem todos os funcionários, terceirizados e gestores (de nada adianta os chefes não serem conscientizados, pois cabe a eles dar o exemplo);

h) criação de um canal de denúncia anônimo;

i) preparar o terreno para a adequada coleta das provas. Nesse sentido, é fundamental guardar os *logs* da rede, guardar os *e-mails* originais (eletrônicos), dados de acesso, entre outros;

j) seguir o “princípio do menor privilégio”, ou seja, garantir acesso ao que é estritamente necessário;

k) ter classificação da informação bem definida e aplicada;

l) realizar testes de vulnerabilidade e simulações de *black bag*³³⁷.

Com a aplicação desses controles, certamente não eliminaremos a atividade do *insider*, mas reduziremos a probabilidade de ocorrência dessa situação e permitiremos pegar o infrator com a mão na máquina, literalmente.

— Barreira 6 — Diagnosticar — aprendizado e fortalecimento do ciclo de segurança. É essencial aprender com o incidente para aumentar o grau de segurança e evitar nova ocorrência.

337. *Black bag* — operações militares de infiltração com objetivo de sabotagem ou furto e/ou extração de pessoas. Simulação de *black bag* é a alocação de um indivíduo, terceiro ou não, para testar tanto a segurança lógica como física e diagnosticar os pontos falhos.

Por último, não podemos esquecer que na Sociedade Digital ainda há muitos conflitos em andamento e que estão por vir devido à queda das barreiras físicas, tornando os países cada vez mais expostos e sujeitos a espionagem por outros. No entanto, tendo em vista a dificuldade que os atacantes encontram para atacar alvos militares e de inteligência, é bastante comum o iniciar em terceiro — normalmente prestador de serviço — e daí fazer o ataque à Instituição alvo³³⁸. De que adianta tomar todas as precauções, mas não ter qualquer recomendação e/ou controle sobre nível de segurança dos terceiros prestadores de serviço para empresa?

Com a baixa cultura de segurança da informação nas empresas, associada à característica solícita do brasileiro, o espião não precisa mais invadir ou interceptar, ele entra pela porta da frente. Precisamos estar mais atentos, sob pena de responsabilidade por negligência e omissão, conforme reza o art. 1.016 do Código Civil brasileiro.

8.49. Paper less e Gestão Eletrônica de Documentos — GED

Vivemos o desafio da sociedade que pretende eliminar o papel como principal suporte de documentação de suas relações. Vivemos em um período de transição para a “paper less society”. Isso implica uma problemática para o Direito no sentido do legado já gerado em papel. Pois a migração de suporte pode ocasionar quebra de integridade, por certo, seja do suporte físico para o digital ou vice-versa. Motivo pelo qual o ideal é tudo já nascer, ser gerado em mídia eletrônica e não haver esta necessidade de materialização e desmaterialização. O processo de digitalização simples pode gerar algum tipo de arguição de quebra de integridade e na necessidade de se fazer prova pericial sempre precisamos do original da manifestação de vontade, conforme observamos na leitura do art. 365 do Código de Processo Civil. Um documento digitalizado não é periciável. Assim como um *e-mail* impresso também não o é. Mas isso pode ser resolvido com a digitalização registrada ou com a digitalização autenticada, feitas por Oficial de Registro de Títulos e Documentos ou por um Notário. Assim, busca-se trazer a fé pública para os casos em que isso seja necessário, em que possa haver algum tipo de impugnação referente a repúdio de autoria ou quebra de integridade.

338. Guerra cibernética — <www.defesanet.com.br/docs/cgsi.pdf>.

Além disso, há o lado do documento que já nasce diretamente na via eletrônica e que exige, cada vez mais, que as empresas façam a sua guarda adequada até mesmo para fins de *e-discovery* (termo que define a apresentação de prova eletrônica perante a Justiça).

Por este motivo, atualmente, tem sido motivo de grande preocupação das empresas a gestão da documentação eletrônica³³⁹, com objetivos de proteção de conhecimento, segurança da informação, bem como para garantir a guarda da prova legal necessária em situações de auditoria ou contencioso.

Apesar de a rotina dos negócios já envolver uma série de relações não presenciais, que geram obrigações e responsabilidades mediante o uso de tecnologia e meios eletrônicos de comunicação, que inclui a troca de mensagens entre executivos, revisão de minutas de contrato com validação e aprovação do documento final, tudo por *e-mail*, são poucas as empresas que possuem uma política claramente definida, ficando muitas vezes a critério dos usuários, ou seja, funcionários de todos os perfis e níveis hierárquicos, a decisão individual sobre o que guardar, como e por quanto tempo, de *e-mail* a documentos digitais confidenciais.

O que fazer se houver uma ordem judicial que exija a apresentação de determinada evidência que estaria em uma caixa postal de *e-mail* e a empresa não tiver mais os dados? Para muitos ainda paira a dúvida se um *e-mail* pode ser considerado um documento, uma prova. No Direito brasileiro, a definição de documento pode ser compreendida como um instrumento de registro de um fato, seja em suporte físico ou eletrônico (onde a sequência de *bits* pode ser traduzida por um programa de computador e representar um fato).

É importante destacar que em todos os ordenamentos jurídicos o conceito de documento está associado ao termo “escrito”. Ou seja, independentemente de que suporte ele esteja fixado, o elemento fundamental é a compreensão inequívoca da manifestação e vontade nele expressa. Nesse sentido, o uso da “tecnologia papel” demonstrou-se uma grande evolução com relação à prova oral, já que facilitou a circulação das obrigações de modo mais autônomo e independente da presença das partes e suas testemunhas. E com a evolução da

339. Conceito de Documento eletrônico — segundo o Decreto italiano n. 513/97, documento eletrônico é “a representação eletrônica (ou digital) de atos, fatos ou dados juridicamente relevantes”. Na mesma direção, a Portaria do Ministério da Fazenda n. 528/96, de 2 de setembro de 1996, publicada no *DOU* em 10-10-1996, que regulamentou o Sistema Setorial de Gestão de Documentação e Informações — SGDI, do Ministério da Fazenda, dispõe que “compreende-se por documento, qualquer que seja o suporte utilizado, o conjunto de informações que registre o conhecimento humano, de forma que possa ser utilizado como elemento de consulta, estudo e prova”.

tecnologia da informação, passou-se a não mais precisar de qualquer suporte físico e tangível³⁴⁰.

Logo, pelo Direito Civil³⁴¹ e Processual Civil brasileiro³⁴², temos que o conceito jurídico de Documento é: a) escrito oficial que identifica uma pessoa; b) instrumento escrito que, juridicamente, faz fé daquilo que atesta, tal como contrato, escritura pública, certificado, atestado, recibo, título etc.; e c) qualquer escrito oferecido em juízo que forneça prova de alegação do litigante.

Ressalte-se que quando falamos de prova eletrônica, a gestão documental deve envolver a guarda de *e-mails*, mas também a guarda de *logs* e metadados que demonstrem a autoria do documento bem como a preservação de sua integridade. Ou seja, como vincular o autor ao conteúdo? No que tange à definição de “originalidade” de um documento, estes dois elementos — autoria e integridade — são fundamentais para que a prova seja forte, ou seja, dificilmente repudiável. A este processo de análise e elaboração da arquitetura legal da informação gerada, manuseada e eliminada pela empresa, chama-se “*Legal Storage Plan*” ou “Gestão Documental”.

Em termos de gestão, de nada adianta guardar a prova se não for possível encontrá-la quando precisar. Por este motivo, tem crescido o uso de tecnologias para gestão eletrônica de documentos, que devem não apenas observar o armazenamento, mas principalmente a segurança do ambiente para proteção da integridade ao longo do tempo e a taxonomia e demais indicadores de localização e identificação da base de dados.

340. A Organização das Nações Unidas, por meio da UNCITRAL, comissão que tem por atribuição o tratamento de questões relativas ao comércio internacional, propôs a edição de Lei Modelo baseada no princípio de equivalência entre suporte físico e digital, da qual destacamos os dispositivos indicados abaixo:

“Art. 6 — Quando a lei requeira que certa informação conste por escrito, este requisito considerar-se-á preenchido por uma mensagem eletrônica se a informação nela contida seja acessível para consulta posterior.

Art. 7 — Quando a lei requeira assinatura de uma pessoa, este requisito considerar-se-á preenchido por uma mensagem eletrônica quando: a) for utilizado algum método para identificar a pessoa e indicar sua aprovação para a informação contida na mensagem eletrônica;

Art. 8 — Existir garantia fidedigna de que se preservou a integridade da informação desde o momento de sua geração em sua forma final e for acessível à pessoa à qual ela deva ser apresentada”.

341. Art. 225 do Código Civil: “As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão”. Ver também arts. 333, 334 e 335.

342. Art. 368 do Código de Processo Civil: “As declarações constantes do documento particular, escrito e assinado, ou somente assinado, presumem-se verdadeiras em relação ao signatário”.

Ressalte-se, por oportuno, que o ordenamento jurídico brasileiro prevê a atribuição de maior força probante aos documentos eletrônicos em razão da Medida Provisória n. 2.200-2, de 24 de agosto de 2001, que institui a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), viabilizando a utilização de ferramentas derivadas da certificação digital. Referido instrumento tem força de lei, conforme disposição contida na Emenda Constitucional n. 32, de 11 de setembro de 2001, já explicitado em outro capítulo do livro.

Independentemente da solução a ser adotada, o importante é que as empresas não podem mais negligenciar a gestão da documentação eletrônica de seus negócios, em uma realidade mais complexa que exige planejamento e guarda adequada das provas jurídicas digitais. Para tanto, a padronização por meio de uma norma é o mais recomendável, e a partir dessa padronização a implementação de algumas medidas, processos e tecnologias que permitam garantir a sua eficácia, devendo estar alinhada com a legislação nacional e melhores práticas de mercado³⁴³.

343. Abaixo o resumo de Legislação e Melhores Práticas de Mercado aplicáveis:

- Constituição Federal de 1988, em especial o art. 5º, IV, V, X, XII, XIV;
- Código Civil, arts. 186, 187, 217, 219, 225 e livro “Das Obrigações”;
- Código de Processo Civil, nos arts. 131, 332, 334, 368, 389;
- Código Penal, em especial em seus arts. 153, 155, 163, 184, 299, 307;
- Código de Processo Penal, arts. 231 e 232;
- Código de Proteção e Defesa do Consumidor, arts. 12 e 14;
- Consolidação das Leis do Trabalho (CLT), arts. 2º, 3º, 482 e outros;
- Lei Federal n. 9.262/96 (Lei de Interceptação);
- Lei Federal n. 973/1903 (registro de títulos e documentos);
- Lei Federal n. 5.433/1968 (microfilmagem) e Decreto n. 1.799/1996;
- Lei Federal n. 6.015/1973 (registros públicos), art. 127, I e arts. 142 e 161;
- Lei Federal n. 8.935/94 (serviços notariais e de registro), arts. 1º, 3º, 6º, 7º, 41;
- Medida Provisória n. 2.200-2/2001 (infraestrutura de chaves públicas);
- Resolução n. 1002/02 do CONFEA (Código de Ética Profissional);
- Lei Modelo da UNCITRAL nos arts. 6º, 7º, 8º;
- ISO/IEC 18044 — Gestão de Incidente de Segurança da Informação;
- ISO/IEC 27001 — Sistema de Gestão de Segurança da Informação;
- ISO/IEC 27002 — Código de Prática para a Gestão da Segurança da Informação (antiga ISO/IEC 17799);
- ISO/IEC 31000 — Gestão de Riscos;
- Demais normas relacionadas, com destaque para o cumprimento de normas técnicas, regulamento profissional e outras de ordem administrativa.

Em termos de necessidade de elaboração de leis específicas, há alguns projetos de lei³⁴⁴ discutindo o tema não apenas da documentação eletrônica, mas também da documentação digitalizada, ou seja, que nasceu, originariamente, no suporte físico e depois migrou para ambiente eletrônico. Este debate legislativo visa trazer maior segurança jurídica para a equiparação do valor probatório do documento digital e seu original físico, permitindo, inclusive, a destruição deles após o processo de digitalização, na mesma linha do que foi feito em 1968 com a Lei de Microfilmagem, que era extremamente visionária para a época em que foi concebida, muito mais do que o são os projetos de lei atuais.

Recentemente, a Lei n. 12.682/2012 foi aprovada (antigo PLC — Projeto de Lei da Câmara — n. 11/2007). Esta norma trata da digitalização de documentos. Aparentemente, parece um avanço, no entanto, os artigos que tratavam sobre o descarte do documento original e que davam ao documento digitalizado o mesmo efeito jurídico conferido ao documento microfilmado foram vetados pela Presidência da República (arts. 2º, 5º e 7º).

A lei não tratou sobre a padronização do procedimento técnico de digitalização, considerando-a uma evolução da Lei n. 5.433/68 e do Decreto n. 1.799/96, que padronizou a microfilmagem. Ao contrário, acabou por gerar um cenário novo, e de certo modo prejudicial, por ser mais custoso, visto que passou a exigir o uso de certificado digital de forma obrigatória no processo de digitalização, mas sem permitir que seja eliminado o original automaticamente.

Partindo do âmbito privado, surgiram diversas iniciativas de autorregulamentação sobre o processo padronizado de digitalização, como pode ser visto no Mercado Financeiro (com o “CompImagem” — compensação de cheque por imagem) e na Saúde, com a Resolução do Conselho Federal de Medicina n. 1.821/2007, que inclusive já aborda procedimento de digitalização.

344. Os projetos de lei com maior destaque são PLS n. 146/2007, do Senador Magno Malta, e o PL n. 1.532/99 da deputada Ângela Guadagnin. Além disso, devemos destacar PLC n. 11/2007 (que nada mais é que o citado PL n. 1.532), que foi desenvolvido com base em um anteprojeto que tem como escopo: “disciplinar a digitalização e o armazenamento em meio eletrônico, óptico ou equivalente, e a reprodução de documentos públicos e privados”. Existe ainda Projeto muito interessante, o PL n. 3.070/08, do Sr. Deputado Paulo Teixeira, que incentiva o uso de formatos abertos para armazenamento e disponibilização digital de todos os documentos de entidades da Administração Pública Direta e Indireta, Autárquica e dos órgãos autônomos e empresas estatais. Fora estes, há ainda: PL n. 3.173/97, PL n. 1.483/99, PL n. 1.589/99, PL n. 4.906/2001, PL n. 6.965/2002, PL n. 7.093/2002, PL n. 7.316/2002, PLS n. 229/2005, PL n. 299/2005, PL n. 288/2007, PL n. 7.709/2007, PLS n. 231/2007 e PL n. 3.070/2008.

Quando se fala em migração de suporte, seja do físico para o eletrônico ou o contrário, o que importa é como estabelecer um procedimento. É importante que, durante o procedimento, seja possível comprovar que não houve alteração do conteúdo do documento durante a mudança de suporte (ou seja, quebra de integridade). Com isso dá-se segurança jurídica ao documento, além de permitir a ele auditoria posteriormente. Mesmo com esse histórico, durante o trâmite do PLC n. 11/2007, o Congresso Nacional entendeu que o texto da lei deveria ser objetivo e que o procedimento fosse regulamentado em norma a parte, como foi com a microfilmagem.

Logo, entre as justificativas do veto — que dizia sobre poder digitalizar e eliminar o original em papel (ou seja, tornar equivalente a imagem digitalizada ao original) — consta justamente a falta de procedimento para a reprodução dos documentos resultantes do processo de digitalização, que era o único elemento que precisava ser discutido em lei, mas não foi.

Lembrando que o Judiciário já aceitava documentos digitalizados sem uso do certificado ICP-Brasil, assim como cópia simples de documentos, conforme previsto no Código de Processo Civil, editado pela Lei n. 11.419/2006, que regula o processo eletrônico e alterou o texto do Código.

No Judiciário há a questão da perícia de autoria (exame grafotécnico na assinatura de documentos e contratos), em que o documento não é descartado e, havendo qualquer questionamento sobre ele, pode-se apresentar o original. Caso tenham decidido pelo descarte, será necessária prova por outros meios (o que ocorre, por exemplo, quando se comprova a obrigação contratada com o comprovante de pagamento-quitação). É importante lembrar que, se o documento original já tinha algum vício, seja em relação à autoria ou em relação ao conteúdo, ele permanece, mesmo após a digitalização, ainda que ela seja com certificado ICP-Brasil.

Diante do exposto, no cenário atual, qual o efeito prático da Lei n. 12.682/2012? Ela não permite de forma expressa o descarte de documentos em papel após a digitalização e apenas favoreceu as empresas que ofertam certificados digitais da ICP-Brasil, gerando ainda dúvidas sobre a aceitação do documento digitalizado sem uso do mesmo.

A lei de digitalização aprovada gera um grande retrocesso para o Brasil. Podemos dizer que o legislador de 2012 ficou mais retrógrado do que o legislador de 1968, que na sua época, sim, quebrou o paradigma do papel, essencial para diminuir o Custo Brasil. Só há um caminho: continuar digitalizando utilizando uma matriz de risco de guarda de originais em papel (contra os originais eletrônicos), associada a uma tabela de temporalidade atualizada,

criando procedimentos padrão por autorregulamentação e esperar que haja um Decreto Presidencial da Presidência da República ou do próximo em exercício a regulamentar a matéria da forma adequada, permitindo a eliminação do papel.

Ainda não foi inventada uma tecnologia a prova de má-fé, mas por certo, na Era em que vivemos, o pior é precisar da prova eletrônica e não ter feito a guarda da mesma. Lembrando que *e-mail* impresso é cópia, o original é o digital e quando envolver coleta de prova publicada na internet, a feitura de Ata Notarial³⁴⁵ é essencial. Logo, podemos concluir que:

- Precisamos pensar em gerar documentos originais puramente eletrônicos;
- A migração deve ser um paliativo para diminuir o legado em papel;
- A Lei n. 12.682/2012 não resolveu a questão do descarte dos documentos antes de encerrar o prazo prescricional;
- É possível fazer a digitalização simples ainda, com base no art. 365, VI, do CPC;
- O uso de um certificado digital tem o condão de garantir que não houve quebra de integridade no processo de digitalização;
- Dependendo do original em papel, após a digitalização o mesmo terá que ser mantido (caso possa haver necessidade de perícia de assinatura, por exemplo), mas se não for esta a hipótese, em muitos casos, poderá ser descartado;
- É essencial elaborar uma Política de Gestão Documental atualizada, prevendo já este contexto eclético de arquivo em papel, digitalizado e com originais eletrônicos;
- Também é fundamental investir em ferramentas de GED para adequada gestão e localização dos documentos guardados de forma eletrônica;
- Precisa criar uma tabela de temporalidade híbrida e treinar os gestores sobre o que guardar, como e por quanto tempo;
- Em geral, quase 60% do que está sendo guardado em papel pode ser descartado, e quase 80% do que está sendo eliminado no eletrônico deveria ser guardado (de *e-mails* originais, a notas fiscais eletrônicas a *logs* de acesso da rede). Precisa fazer planejamento técnico-jurídico;
- Precisa haver padronização do processo de digitalização (como ocorreu com a microfilmagem) e isso pode ser feito por autorregulamentação de mer-

345. Ata Notarial — Lei n. 8.935/94.

cado e eventualmente ser consolidado através de um Decreto Presidencial que possa regulamentar isso (como foi feito em 1996 no Governo FHC), permitindo a eliminação do papel após a digitalização. Ou então, precisaremos de uma nova lei, já que a atual mais regrediu do que avançou no tema.

8.50. Seguro de Risco Eletrônico

A introdução das Tecnologias da Informação nos negócios é uma tendência já consolidada no sentido de trazer agilidade nas decisões e nas comunicações, muitas vezes em tempo real, com ganhos de custo. Em verdade poucas empresas podem-se dar ao luxo de prescindir de manter uma página atualizada na Internet ou de utilizar o *e-mail* nas comunicações mais corriqueiras. Muitas já precisam operar no regime 24/7 (24 horas por dia e 7 dias por semana). Mas como fazer se a empresa sair do ar?

Devido ao crescimento de incidentes relacionados com a segurança da informação, muitas Seguradoras têm começado a excluir riscos associados a estas questões de Segurança e TI, criando lacunas em apólices tradicionais, o que acaba por gerar dentro do ambiente empresarial a incerteza da proteção do seguro.

Por causa desta “incerteza”, muitas empresas têm optado pela “aceitação implícita” desses tipos de riscos como sendo do próprio negócio. Ocorre que estes riscos constituem um passivo difícil de calcular e que pode inviabilizar uma série de operações que deveriam ser vantajosas para as empresas. No entanto, como já aconteceu anteriormente, há quem comece a propor um “seguro para riscos eletrônicos”. Mas isso é viável?

Em princípio, um seguro desta natureza deveria tratar especificamente dos riscos associados à Tecnologia da Informação, separando em duas categorias — empresas que usam a tecnologia para conseguir executar suas atividades, e empresas já de tecnologia ou nascidas na nova economia (como provedores, desenvolvedores, lojas virtuais, outros).

Este tipo de seguro deve ter uma apólice bem detalhada para inclusive abranger situação de cobertura em hipótese de indenização de danos a terceiros causados por mau uso das novas tecnologias, como *e-mail* e Internet, conforme passamos a analisar em detalhes.

Mas por que este tipo de seguro ainda não recebeu ampla aceitação? Talvez pelo fato de, em muitas apólices que existem no mercado, a cobertura depender de que haja ação judicial entre as partes. Mas que empresa vai querer ter este tipo de exposição para conseguir acionar o seguro? Ainda mais se tiver

sido por um motivo de “invasão de *hacker*”, “infração de privacidade ou sigilo de dados”?

Normalmente as coberturas tratam de: a) indenização a terceiros, que seria a responsabilidade civil relacionada a comunicações por meio eletrônico; b) responsabilidade civil profissional, devido a ato danoso cometido no curso das atividades comerciais da empresa, envolvendo uso de sistemas, ataque de *hacker* e vírus; c) reclamações apresentadas por qualquer empregado da empresa segurada, inclusive sobre discriminação, invasão de privacidade, quebra de confidencialidade dos registros mantidos sobre o mesmo; d) prejuízos sofridos pelo segurado no tocante a danos ocorridos nos sistemas do segurado, interrupção de atividades por ataque de *hacker* ou vírus, uso do sistema de informática para subtrair recursos (furto, fraude), modificação, destruição ou entrada fraudulenta de dados eletrônicos, situação de ameaça ou extorsão considerando introdução de um ataque de *hacker*, vírus, disseminação, divulgação ou utilização de informações contidas nos sistemas do segurado, ou em seus equipamentos (*notebook*, *pen drive*, *smartphone*); e) custos judiciais relacionados ao ataque a direitos de propriedade intelectual do *website*; f) proteção de marca na internet.

Há uma complexidade adicional para se contratar um seguro de riscos eletrônicos devido à necessidade de a empresa ter uma análise de vulnerabilidades do seu ambiente para definir adequadamente o valor do prêmio e das coberturas.

Logo, é um produto de difícil venda, pois exige customização e o mercado ainda não compreende muito bem quais são os riscos eletrônicos e que situações a cobertura vai atender e quais não. Como se sabe, o custo de um seguro (prêmio) está diretamente relacionado com a extensão dos danos cobertos, bem como com a frequência histórica ou presumida dos eventos de sinistro. Assim, quanto mais uma empresa conhece os seus processos internos maior será a possibilidade de atuar no sentido de sua otimização e eficaz implantação das medidas de segurança e com isso o custo de um seguro para proteger a continuidade das suas operações é sensivelmente reduzido.

Além do seguro de riscos eletrônicos, há duas outras modalidades de seguro que tem crescido muito nos últimos anos: o E&O (do inglês *Errors & Omissions*) e o D&O (do inglês *Directors & Officers*)³⁴⁶.

346. Segundo informações coletadas junto ao especialista André Lellis Werneck, da AON (www.aon.com.br), as principais garantias desses seguros envolvem cobertura para:

• Reclamações nas quais o Segurado seja demandado por débitos tributários, trabalhistas,

O E&O tem como objetivo garantir o Patrimônio da Firma, Sócios e Praticantes, ameaçado com a reparação danos de grande monta, caso cometam falhas no exercício da profissão. A contratação de uma apólice como esta também serve como uma garantia financeira para os clientes, afinal o risco assumido pelo advogado pode ser superior à sua capacidade financeira. Tem o objetivo de indenizar as perdas financeiras sofridas pelos clientes do escritório em decorrência de erros e omissões profissionais dos advogados e paralegais. Os segurados são as pessoas dos advogados e a pessoa jurídica do escritório. Para que haja cobertura, o advogado deve estar agindo de acordo com a regulamentação da OAB, excluindo-se, portanto, as atividades não inerentes à categoria.

Já o D&O tem o objetivo de garantir o Patrimônio dos Sócios e Administradores da Sociedade, ameaçado com reparação de danos de grande monta, caso cometam falhas na gestão do próprio escritório e das empresas nas quais são procuradores. A apólice visa proteger o patrimônio pessoal das pessoas físicas que exercem cargos de gestão em pessoas jurídicas. Todos os adminis-

previdenciários, da empresa onde atua.

- Reclamações de quaisquer credores da empresa Tomadora do Seguro contra o Segurado (administradores).
- Reclamações que a própria empresa Tomadora do seguro possa mover contra os Segurados (diretores, membros de conselho, executivos em geral).
- Reclamações que os sócios ou acionistas da empresa Tomadora possam mover contra os Segurados, independentemente do percentual de ações ou cotas detido por cada um.
- Garantia expressa de cobertura de despesas de defesa para processos nos quais se discute um possível Ato Doloso do Segurado (Civil e Criminal).
- Reclamações contra os Segurados decorrentes da desconsideração da personalidade jurídica da empresa Tomadora do Seguro.
- Reclamações contra os Segurados decorrentes de danos corporais sofridos por empregados e terceiros, relacionados às atividades da empresa.
- Limite especial de cobertura para processos de natureza Ambiental movidos contra os Segurados.
- Processos de natureza administrativa contra os Segurados (inclusive órgãos governamentais reguladores e fiscalizadores, Tribunais de Contas, Inquéritos Policiais etc.).
- Reclamações contra os Segurados em virtude de erros e omissões na prestação de serviços profissionais da empresa.
- Penalidade de multa administrativa ou contratual contra os Segurados (somente Custos de Defesa, incluindo depósitos judiciais ou administrativos, reembolsável em caso de condenação).
- Demais situações onde o Segurado possa ser pessoalmente responsabilizado em virtude da posição que ocupa na empresa Tomadora, exceto os riscos excluídos.

tradores, tais como conselheiros, diretores, gerentes, supervisores e equivalentes que detenham poderes que impliquem o exercício de tomada de decisões e autoridade diretiva na Empresa estão garantidos, em apólice aberta (não nominal). A cobertura é extensiva a cônjuges, herdeiros, representantes legais e espólio. Este tipo de seguro tem sido muito contratado para empresas que fazem abertura de capital na bolsa de valores, bem como para executivos de linha de frente como CEO (*Chief Executive Officer*), CFO (*Chief Financial Officer*), CIO (*Chief Information Officer*).

Independentemente de se ter um seguro ou não, o gerenciamento de riscos digitais passa necessariamente pelas seguintes etapas: a) adequação à legislação vigente aplicável em toda a cadeia do negócio; b) revisão de contratos com fornecedores, parceiros, colaboradores e clientes; c) elaboração de novas minutas de contratos que tratem adequadamente das responsabilidades das partes quanto aos riscos digitais envolvidos, incluindo aplicação de cláusulas ou acordos de nível de serviço (SLA) e Plano de Continuidade (PCN); d) implantação de políticas de segurança para o uso das ferramentas tecnológicas no trabalho; e) conscientização para construção de cultura interna na empresa de segurança da informação e proteção dos ativos intangíveis.

Uma vez que o patrimônio e a riqueza da Sociedade Digital está em dados, é preciso protegê-los, e para o que não se pode evitar, deve-se ter um seguro.

8.51. Segurança Pública Digital

A Segurança Pública Digital visa a prevenção e o combate dos novos tipos de ameaças e crimes resultantes de um cenário de integração de mundo real e cibernético. Dentro dessa linha evolutiva do pensamento da segurança em uma realidade mais digital houve a criação do NATO Cooperative Cyber Defense Centre of Excellence, que surgiu após o ataque cibernético ocorrido na Estônia, quando instituições públicas e privadas solicitaram à OTAN para realizar uma pesquisa para abordar a cyberdefesa.

Em princípio, a Segurança Pública Digital apoia no planejamento estratégico do combate às seguintes ameaças: cyber-terrorismo, ataques a *sites* públicos, espionagem eletrônica entre países e instituições, fraude eletrônica (ataques a bancos e clientes do mercado financeiro), *identity thiefs* e estelionato digital (falsa identidade digital, uso de dados de terceiros, clonagem de cartão de crédito), tráfico de entorpecentes e pedofilia na internet e nas mídias sociais.

Alguns dos países que já regulam e atuam mediante uma estrutura de Segurança Pública Digital são a Austrália, a União Europeia, a Nova Zelândia, a Rússia, o Canadá, a França, a Alemanha, o Reino Unido, a República Tcheca, a Estônia, a Polônia, o Japão, os EUA e a África do Sul.

No caso do Brasil, apesar de em 2012 ter sido lançado o Centro de Defesa Cibernética (CDCiber — órgão do Exército Brasileiro), esse tipo de estrutura mais convergente e holística ainda deve ser criada, principalmente devido à realização de eventos de grandes proporções, como a Copa do Mundo e as Olimpíadas. Imagine como ficaria o tratamento de um *post* no *Facebook* em que a pessoa diz que tem uma bomba no estádio? Justamente para definir um fluxo de ação responsável, com prazos, como obter provas rápidas junto a terceiros é que tem que haver um Plano de Segurança Pública Digital estabelecido.

Segundo a Secretaria de Assuntos Estratégicos, no tocante ao acordo de Cooperação Russa, as principais potenciais ameaças cibernéticas no campo da Segurança das Informações são:

- bloqueio e desinformação em recursos de informação e telecomunicação;
- ação de guerra ou terrorista contra fluxo de informação em estruturas vitais;
- desestabilização da sociedade por meio da manipulação da consciência da população;
- adoção de doutrinas e políticas, individualmente, pelas nações com respeito à segurança das informações, provocando uma corrida armamentista;
- uso de recursos de TI em detrimento dos direitos humanos e da liberdade de acesso à informação;
- a disseminação generalizada de informação, violando os princípios e as normas da legislação internacional;
- o desenvolvimento de conceitos e meios por países membros, visando à guerra cibernética.

Com isso, foi estabelecido um plano de defesa cibernética, que soma também as iniciativas de segurança pública. Ou seja, não adianta apenas gerar a proteção de fronteiras da informação para fora, visto que muitas ameaças podem ocorrer provocadas por indivíduos de dentro do próprio país.

O plano visa melhorar a interoperabilidade de defesa cibernética dentro da capacidade do ambiente da rede da OTAN Enabled (NNEC), projetar o desenvolvimento da doutrina e do conceito de defesa cibernética e sua validação. Além disso, reforça a Segurança da Informação e a defesa cibernética

com educação, conscientização e treinamento, fornecendo apoio à defesa cibernética para a experimentação (incluindo *on-site*) e analisando os aspectos jurídicos da defesa cibernética.

Logo, deve existir uma convergência (união) entre Defesa Cibernética (âmbito mais militar e de agências especiais — fronteiras físicas e fronteiras digitais) e a Segurança Pública Digital (que acaba abrangendo uma parcela do Poder de Polícia — comportamento dos indivíduos no ambiente digital). Devemos destacar que muitas das ameaças digitais ainda não são consideradas crimes tipificados na legislação brasileira. Por isso, precisa-se receber tratamento diferenciado, como já visto no capítulo específico sobre crimes digitais. Seja para fazer um vírus de computador ou tirar do ar um *site*, ainda há muitas lacunas a serem tratadas do ponto de vista legislativo que podem dificultar a punição mais severa dos infratores.

Por isso, um dos trabalhos mais importantes da Segurança Pública Digital envolve a prevenção das ameaças, com campanhas maciças para a população e com canais de denúncia anônima para obter maior celeridade no tratamento, resposta e contenção das mesmas. Deve haver um interlocutor com a Sociedade Civil, como, por exemplo, a figura de um “Secretário de Segurança Pública Digital”, que possa manter esse diálogo permanente e gerar uma base de conhecimento que permita avançar no tocante à proteção digital.

A Segurança Pública é uma atividade pertinente aos órgãos estatais e à comunidade como um todo, realizada com o fito de proteger a cidadania, prevenindo e controlando manifestações da criminalidade e da violência, efetivas ou potenciais, garantindo o exercício pleno da cidadania nos limites da lei. O Poder de Polícia abrange atividade da Administração Pública, expressa em atos normativos ou concretos, que condicionam a liberdade e a propriedade dos indivíduos. Ou seja, é uma ação fiscalizadora, preventiva ou repressiva, com imposição coercitiva aos particulares de um dever de abstenção (não fazer), para conformar os particulares os comportamentos aos interesses sociais consagrados no sistema normativo.

Os principais valores que estão inseridos no Poder de Polícia de um Estado e que têm relação direta com a Segurança Pública Digital são: proteção da ordem pública, da tranquilidade pública, da moralidade pública e da economia popular, tendo como objetivos garantir o bem-estar social, evitar um dano — como regra, o poder de polícia não pretende uma atuação no particular, mas uma abstenção exigindo uma obrigação de *não fazer*, prestando um serviço público —, oferecer comodidade ou utilidade aos cidadãos (utilidade coletiva), vedar um comportamento e evitar uma consequência antissocial.

Para que o Poder de Polícia cumpra com sua missão respeitando os direitos civis, deve sempre utilizar meios coativos atendendo ao princípio da proporcionalidade, atuando com cautela. Em hipótese alguma deve se servir de meios mais energéticos que os necessários à obtenção do resultado pretendido pela lei (risco de abuso e responsabilidade administrativa), devendo utilizar o meio coativo somente quando não houver outro meio eficaz para o cumprimento da pretensão jurídica.

Por certo há um paradoxo natural entre segurança e privacidade. Por isso, quanto maior a necessidade de proteção de um povo na era digital, maior a necessidade de se poder ter acesso a provas eletrônicas geradas em dispositivos tecnológicos particulares ou de terceiros. Um criminoso não carrega mais a prova anotada em um papel no bolso, mas sim em seu celular, *pen drive*, *notebook*, perfil na rede social, caixa postal de *e-mail* gratuita, entre outros. Por isso, na Segurança Pública Digital faz-se essencial ter procedimentos específicos para a realização de revista digital, como já ocorreu em Londres, nas Olimpíadas de 2012, em que policiais podiam coletar dados do celular de posse ou propriedade do suspeito no momento da averiguação. Segundo Celso Antônio Bandeira de Mello³⁴⁷, há duas polícias:

Administrativa — preventiva e repressiva — atua para impedir ou paralisar atividades antissociais quando o interesse público já tiver sido violado;

Judiciária — repressiva — atua para preordenar a responsabilização dos violadores da ordem jurídica.

É importante ressaltar que a Administração pública, no exercício da polícia administrativa, age repressivamente. Sempre que obsta a atividade particular já em curso, é porque esta se revelou contrastante com o interesse público, isto é, lesou, causando um dano para a coletividade. Exemplo: a dissolução de um comício, de uma passeata, atos típicos da polícia administrativa, tem lugar apenas quando se revelam perturbadores da tranquilidade pública, isto é, quando já veriam o interesse protegido pelo poder de polícia e, em consequência, já causaram um dano, uma perturbação, à coletividade.

A atuação administrativa é marcada, aí, pela repressão a uma atuação antissocial. Só se poderá considerá-la preventiva relativamente, isto é, em relação aos futuros danos dos outros que adviriam da persistência do comportamento reprimido.

347. BANDEIRA DE MELLO, Celso Antônio. *Curso de direito administrativo*. 29. ed. São Paulo: Malheiros, 2012.

As hipóteses de executoriedade das medidas de polícia administrativa se dão quando: a lei expressamente autorizar; quando a adoção da medida for urgente para a defesa do interesse público e não comportar as delongas naturais do pronunciamento judicial sem sacrifício ou risco para a coletividade; quando inexistir outra via de direito capaz de assegurar a satisfação do interesse público que a Administração Pública está obrigada a defender em cumprimento à medida de polícia.

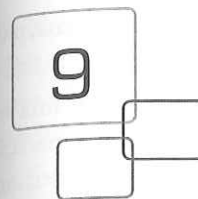
Por certo, não se exclui a possibilidade de recorrer ao Poder Judiciário para sustar as providências administrativas que tenham fundado receio de vir a sofrer desconformidade com a lei para obter as reparações devidas quando, da atuação ilegal da Administração, venham a sofrer danos causados a pretexto do exercício do poder de polícia. Mas é essencial poder agir rápido nos incidentes digitais, e isso exige ter muito mais autonomia. Não dá para esperar a ordem judicial para obtenção dos dados do número do IP junto ao *Facebook* naquele exemplo que demos da bomba no estádio. Tem que ser possível verificar de imediato e se possível pegar o criminoso literalmente com a mão na máquina!

As bases legais que permitem a criação de uma Agência de Segurança Pública Cibernética ou Digital já existem no Brasil:

- Constituição Federal de 1988, art. 91;
- Lei n. 8.153, de 11 de abril de 1991 — regulamenta o art. 91 da CF;
- Lei n. 10.683, de 28 de maio de 2003 — dispõe sobre o funcionamento da Presidência da República e dos Ministérios; art. 6º, inciso IV — responsabilidade do GSI em Segurança da Informação, art. 27 — exceção ao artigo acima, pois o seguimento militar é específico;
- Diretriz Ministerial do Ministério da Defesa n. 14 — designou uma força responsável para cada setor estratégico, com o propósito de coordenar as ações em cada um dos setores. Espaço cibernético — cuida do setor cibernético;
- Decreto n. 5.772, de 8 de maio de 2006 — aprova a estrutura regimental do GSI/PR;
- Lei n. 11.754, de 23 de julho de 2008 — Ministério da Defesa;
- Competências do SENASP — Secretaria Nacional de Segurança Pública:
 - I — assessorar o Ministro de Estado na definição, implementação e acompanhamento da Política Nacional de Segurança Pública e dos Programas Federais de Prevenção Social e Controle da Violência e Criminalidade;
 - II — planejar, acompanhar e avaliar a implementação de programas do Governo Federal para a área de segurança pública;
 - III — elaborar propostas de legislação e regulamentação em assuntos de segurança pública, referentes ao setor público e ao setor privado;

- IV — promover a integração dos órgãos de segurança pública;
- V — estimular a modernização e o reaparelhamento dos órgãos de segurança pública;
- VI — promover a interface de ações com organismos governamentais e não governamentais, de âmbito nacional e internacional;
- VII — realizar e fomentar estudos e pesquisas voltados para a redução da criminalidade e da violência;
- VIII — estimular e propor aos órgãos estaduais e municipais a elaboração de planos e programas integrados de segurança pública, objetivando controlar ações de organizações criminosas ou fatores específicos geradores de criminalidade e violência, bem como estimular ações sociais de prevenção da violência e da criminalidade.

Por não estarmos em estado de guerra nem em estado de sítio, a autoridade pública deve garantir a segurança, mas ela não deve reprimir as liberdades constitucionais já estabelecidas. Os papéis da Segurança Pública Digital devem ser justamente os de assumir o compromisso de não ultrapassar os limites do Poder de Polícia, evitar arbitrariedade, ser o interlocutor com a Sociedade Civil e garantir esse equilíbrio, tendo em vista o respeito às Leis, em especial para proteger a liberdade de expressão, o direito à privacidade e a vedação ao anonimato.



Responsabilidade Civil e Dano Moral no Direito Digital

Em primeiro lugar, a responsabilidade civil é um fenômeno social. Para o Direito, um dos principais pressupostos da responsabilidade civil é a existência de nexo causal entre o ato e o dano por ele produzido. Muito mais importante que o ato ilícito que causou o dano é o fato de que esse dano deve ser ressarcido¹.

O Direito Digital, por sua necessidade de dinamismo, introduz algumas modificações dos conceitos tradicionais de responsabilidade civil no âmbito jurídico. Por isso é importante fazer uma breve revisão no conceito tradicional para então introduzirmos suas modificações.

No Direito tradicional, o conceito de Responsabilidade Civil² adota duas teorias: a teoria da culpa³ e a teoria do risco⁴. A principal diferença entre elas

1. Arts. 186 e 927 do Código Civil.

2. Vide Código Civil, arts. 186, 188, 389 e 927.

3. Trata-se da responsabilidade extracontratual ou aquiliana (derivada da *lex Aquilia*), na qual, para que exista a obrigação de reparar o dano, deve-se poder imputar a quem arcar com o pagamento da indenização, culpa, ainda que levíssima. Este é o princípio que norteia o art. 186 do Código Civil.

4. Álvaro Villaça Azevedo, na sua obra *Teoria geral das obrigações*, subdivide a responsabilidade extracontratual objetiva, na qual aquele que fica obrigado a indenizar não pode ser imputada a culpa pelo dano, em dois tipos: a responsabilidade extracontratual objetiva pura e a impura. A primeira só poderia ser estipulada por lei, nunca por interpretação judicial, e obrigaria o responsável, segundo a lei, a indenizar meramente pela ocorrência do fato, sem cogitar a culpa

está na obrigatoriedade ou não da presença da culpa, mesmo que levíssima, para caracterizar a responsabilidade e o dever de indenizar.

Para o Direito Digital, a teoria do risco tem maior aplicabilidade, uma vez que, nascida na era da industrialização, vem resolver os problemas de reparação do dano em que a culpa é um elemento dispensável, ou seja, onde há responsabilidade mesmo que sem culpa em determinadas situações, em virtude do princípio de equilíbrio de interesses e genérica equidade.

Considerando apenas a Internet, que é mídia e veículo de comunicação, seu potencial de danos indiretos é muito maior que de danos diretos, e a possibilidade de causar prejuízo a outrem, mesmo que sem culpa, é real. Por isso, a teoria do risco atende às questões virtuais e a soluciona de modo mais adequado devendo estar muito bem associada à determinação legal de quem é o ônus da prova em cada caso.

No Direito Digital, a responsabilidade civil tem relação direta com grau de conhecimento requerido de cada prestador de serviço e do consumidor-usuário também. Nenhuma das partes pode alegar sua própria torpeza para se eximir de culpa⁵ concorrente.

Um dos pontos mais importantes é o da responsabilidade pelo conteúdo. Considerando que é o conteúdo⁶ que atrai as pessoas para o mundo virtual e que ele deve estar submetido aos valores morais da sociedade e atender aos critérios de veracidade, é importante determinar os limites de responsabilidade dos provedores, dos donos de *websites*, das produtoras de conteúdo, dos usuários de *e-mail* e de todos os que tenham de algum modo participação, seja em sua produção, seja em sua publicação.

Uma solução para esta questão é determinar uma norma-padrão pela qual, em princípio, os responsáveis pelo conteúdo publicado em um *website* são seus proprietários ou quem eles indicarem como responsáveis editoriais. Cabem aqui as mesmas normas utilizadas para o conteúdo jornalístico convencional.

do agente. A segunda poderia ser objeto de interpretação jurisprudencial, e se refere à responsabilização por atos culposos de terceiro que está vinculado à atividade do indenizador. Dessa maneira não se discutirá, também, a culpa de quem deve indenizar, porém contará este com um direito de regresso para demandar do terceiro que agiu culposamente a composição dos danos que sofreu.

5. Código Civil, art. 150: "Se ambas as partes procederem com dolo, nenhuma pode alegá-lo para anular o negócio, ou reclamar indenização".

6. Lei n. 5.250/67 (Lei de Imprensa), art. 49: "Aquele que no exercício da liberdade de manifestação do pensamento e de informação, com dolo ou culpa, viola direito, ou causa prejuízo a outrem, fica obrigado a reparar".

No entanto, dada a falta de legislação específica sobre o tema, por vezes os Tribunais pátrios promulgam decisões contraditórias. Isto é, ainda se discute uma clara definição dos limites da responsabilidade civil e/ou criminal dos provedores e *sites* que colocam no "ar" conteúdo ilícito adicionado por terceiros.

Em outros termos, devem tais provedores responder por conteúdo do qual não tinham prévio conhecimento? Melhor dizendo, devem os responsáveis por tais provedores responder por atos ilícitos cometidos em seus domínios independentemente de culpa? Tais questões suscitam muitas dúvidas. Esperar, por exemplo, que a empresa Google monitore todos os vídeos postados em seu sítio eletrônico "YouTube", de maneira prévia, é tarefa hercúlea e humanamente impossível.

Contudo, ao ser comunicada, seja por uma autoridade, seja por um usuário, de que determinado vídeo/texto possui conteúdo eventualmente ofensivo e/ou ilícito, deve tal empresa agir de forma enérgica, retirando-o imediatamente do ar, sob pena de, daí sim, responder de forma solidária juntamente com o seu autor ante a omissão praticada (art. 186 do CC)⁷.

O Tribunal de Justiça do Estado de São Paulo, nos autos do Processo n. 988/2006 (Apelação n. 1117060-0/7), julgado em 27-8-2007, confirmou decisão de 1ª Instância, isentando de responsabilidade *site* de leilão virtual por fraude perpetrada por terceiro que, apresentando-se como vendedor, enviou *e-mail* fraudulento, o que fez com que o comprador acreditasse que a mercadoria já estivesse disponível e, com isso, efetuou o depósito correspondente. Ocorre que a mercadoria nunca foi entregue. Entretanto, quando da decisão, levou-se em consideração o fato de o comprador não ter observado todas as recomendações de segurança indicadas no *site*, efetuando, inclusive, depósito do dinheiro em conta corrente de terceiro que não o vendedor da mercadoria. Nesse sentido também entendeu o Tribunal de Justiça do Estado do Rio de Janeiro, quando do julgamento da Apelação Cível n. 2008.001.16030.

Em sentido oposto, a 2ª Turma Recursal dos Juizados Especiais Cíveis e Criminais do Distrito Federal, nos autos do Processo n. 2006.01.1.096659-8, em caso similar, aplicou a chamada "teoria do risco da atividade" e responsabilizou o mesmo *site* de leilão virtual por fraude cometida por terceiro, contra o consumidor. A Turma entendeu que o *site*, ao não demonstrar que a fraude tinha se dado por culpa exclusiva do consumidor ou do terceiro, deveria ser responsabilizado objetivamente, isto é, independentemente da demonstração

7. Código Civil, art. 186: "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

de culpa. Outro dado interessante do teor dessa decisão diz respeito ao fato de que a responsabilidade objetiva foi fundada, além da adoção da teoria do risco da atividade, em razão da violação do dever de preservação de informação restrita ou sigilosa, pelo *site*. Nessa mesma linha, em 18-12-2007, também entendeu a 3ª Turma Recursal Cível dos Juizados Especiais Cíveis do Estado do Rio Grande do Sul, no julgamento do Recurso n. 71001433564, por vislumbrar a existência do dever de indenizar do *site* intermediador que disponibiliza o leilão virtual, em razão da existência de responsabilidade objetiva decorrente do risco do próprio negócio, qual seja, intermediação de compra e venda de mercadorias.

Desse modo, apesar de não haver entendimento jurisprudencial pacífico sobre o tema, ao nosso ver, os limites da responsabilidade sobre o conteúdo devem variar de acordo com o sujeito que detém a obrigação pelo seu fornecimento ou por sua verificação. Na verdade, há o envolvimento quase que concorrente do *website* e do provedor que publica a página no ar, podendo haver a participação de terceiros, prestadores de serviços de fornecimento de conteúdo específico, como já ocorre na área editorial de notícias *online*⁸.

Citamos outro caso prático, em que o Tribunal de Justiça do Estado do Rio Grande do Sul, nos autos do Processo n. 70022511836, em decisão polêmica, mas muito bem fundamentada, condenou um grande provedor de internet pela divulgação de informações difamatórias veiculadas por terceiros em seu serviço de aproximação de pessoas. Novamente, aqui, adotou-se a teoria do risco da atividade. Este é o entendimento atual do Superior Tribunal de Justiça⁹.

Uma decisão que também merece menção, até pelo seu caráter inovador, foi proferida pelo Tribunal do Rio Grande do Sul, nos autos do Processo n. 70009993692. Nela, o Tribunal reconheceu que não possui o provedor de internet responsabilidade pelo conteúdo ilícito colocado no “ar” por terceiros.

8. CDC, art. 51: “São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: I — impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor por vícios de qualquer natureza dos produtos serviços ou impliquem renúncia ou disposição de direitos. Nas relações de consumo entre o fornecedor e o consumidor-pessoa jurídica, a indenização poderá ser limitada em situações justificáveis”.

9. “Civil e consumidor. Internet. Relação de consumo. Incidência do CDC. Gratuidade do serviço. Indiferença. Provedor de conteúdo. Fiscalização prévia do teor das informações postadas no *site* pelos usuários. Desnecessidade. Mensagem de conteúdo ofensivo. Dano moral. Risco inerente ao negócio. Inexistência. Ciência da existência de conteúdo ilícito. Retirada imediata do ar. Dever. Disponibilização de meios para identificação de cada usuário. Dever. Registro do número de IP. Suficiência” (Recurso Especial 1.186.616/MG — 2010/0051226-3 — rel. Min. Nancy Andrighi, DJ 23-8-2011, DOU 31-8-2011).

Entretanto, em razão da impossibilidade de se determinar o autor da matéria ofensiva, deveria o provedor, no caso, responder por ela.

Como podemos observar, as decisões ainda são, por vezes, conflitantes, até porque nos encontramos em uma fase embrionária da Internet no tocante à responsabilização pelo conteúdo veiculado por terceiros.

Novamente, acreditamos que o próprio mercado tende a se autorregular no momento em que os *websites* que não tenham responsáveis editoriais percam credibilidade, determinando que serão os consumidores da informação os principais controladores da qualidade do conteúdo que querem acessar e os principais responsáveis por sua denúncia junto às autoridades no caso de qualquer lesão.

Quanto ao dano moral¹⁰, há muitas controvérsias da matéria no próprio

10. Constituição Federal de 1988, art. 5º, V e X; Código de Defesa do Consumidor, art. 12, e Código Civil, arts. 186 e 927. Jurisprudências relacionadas aos temas:

“Relação de consumo. Responsabilidade civil. Ação de obrigação de fazer. Danos morais. Internet. Provedor de acesso. Legitimidade. Google. Sítio de relacionamento (Orkut). Criação de perfil falso. Terceiro. Mensagens ofensivas a integrantes da comunidade a que pertence o autor. Antecipação de tutela. Retirada do sítio falso. Indenização. Descabimento. Preliminar de ilegitimidade passiva *ad causam* que se acolhe apenas em relação ao corréu, M.P.M.L. Ltda., o qual se limita a somente prestar serviços de proteção à marca ‘Google’ como agente de propriedade industrial. O Google Brasil Internet Ltda., que faz parte do mesmo grupo empresarial da Google, Inc., é parte legítima para figurar no polo passivo da ação indenizatória que tem como fundamento ato ilícito praticado nos domínios do sítio eletrônico denominado Orkut, de que é proprietário. Através desse serviço, os usuários criam páginas pessoais (‘perfis’) a partir das quais se comunicam com os demais e participam de diversas comunidades. Ainda que o serviço, que é objeto da ação, seja prestado envolvendo provedores de acesso à Internet ou responsáveis por sites de relacionamento e os respectivos usuários, não sendo direta ou indiretamente remunerado, aplica-se a legislação consumerista. Aquele que é prejudicado por defeito ou falha na prestação de serviços, tendo ou não relação jurídica direta com o fornecedor, qualifica-se como consumidor (art. 17 da Lei n. 8.078/90). Fato de terceiro. As páginas de relacionamento são marcadas pelo dinamismo, pelo amplo e irrestrito acesso a qualquer indivíduo em qualquer parte do mundo e, consequentemente, pela ausência de qualquer formalidade prévia. Página fraudada por terceiro de molde a conter informações ofensivas ao usuário ou a integrantes da mesma comunidade no Orkut, como se as mesmas tivessem sido criadas e/ou remetidas por este. Circunstância *sui generis* a envolver nova tecnologia e novas relações interpessoais. A possibilidade de identificar o usuário que enviou as mensagens falsas em nome do autor, através do IP (*Internet Protocol*), nem sempre é suficiente para identificar quem seria o real ofensor. Lado outro, inexistindo dever legal ou contratual de monitoramento prévio ou fiscalização antecipada do conteúdo das páginas pessoais, de modo a controlar esse conteúdo e impedir a prática de atos ilícitos (como a adulteração de dados), ou inquinados (como a irrogação de injúrias, calúnias e difamações), por outros usuários ou terceiros, afasta o dever de indenizar. Sem a comprovação do defeito do serviço perde-se um dos requisitos imprescindíveis para a caracterização da responsabilidade civil objetiva (art. 14 da citada Lei n. 8.078/90), sendo certo que a responsabilidade do provedor de acesso e responsável pelo *site* de relacionamento se circunscreve à disponibilização da tecnologia que permite o acesso à WEB. Harmonização do direito à imagem com o preceito que assegura

a livre manifestação do pensamento e da informação vedando, entretanto, o anonimato nas livres manifestações de pensamento (art. 5º, inc. X e art. 5º, inc. IV, IX e XIV, da CRFB/88). Provedor de hospedagem que não está obrigado a fiscalizar, nem realizar qualquer censura prévia ou genérica (o que avilta, ademais, os princípios democráticos insculpidos na Constituição vigente), sobre o conteúdo inserido pelos usuários. Diante da impossibilidade de fiscalizar todas as páginas criadas, e ainda, observando a garantia fundamental do livre pensamento, se torna impossível a exclusão do nome da agravada, sem que esta identifique as respectivas URL (Localizador de Recursos Universal). Ausência de conduta culposa pelo réu, pois não restou evidenciada a negligência, a imprudência ou imperícia. Sentença mantida. Recurso a que se nega provimento" (TJRJ, Agravo de Instrumento 0374854-06.2008.8.19.0001 (2009.001.69800), rel. Mario Assis Gonçalves, j. 22-6-2010).

"Ação de indenização. Dano moral. Orkut. Rede social. Sítio de relacionamento. Internet. Provedor de serviços de informações. Responsabilidade por fato do serviço. Direito do consumidor. Responsabilidade objetiva. Usuário vítima do evento. Ofensas de cunho moral. Expressão 'fazendo a fila andar'. *Quantum*. (...) A relação entre os provedores e usuários da internet é regida pelas normas do Código de Defesa do Consumidor. Os provedores se enquadram como fornecedores de serviços (...) A expressão 'fazendo a fila andar' aposta por usuário inidôneo na denominação do perfil pessoal da usuária atinge a sua honra subjetiva. A expressão 'fazer a fila andar', no jargão popular, significa sucessão de parceiros amorosos, denotando promiscuidade por meio de relacionamento sexual não monogâmico, ou seja, com muitos parceiros diferentes" (TJMG, Recurso 1.0145.08.471404-0/001(1), rel. Cabral da Silva, j. 3-8-2010).

"Mãe é condenada por *cyberbullying* praticado por filho menor. Apelação. Responsabilidade civil. Internet. Uso de imagem para fim depreciativo. Criação de *flog* — página pessoal para fotos na rede mundial de computadores. Responsabilidade dos genitores. Pátrio poder. *Bullying*. Ato ilícito. Dano moral *in re ipsa*. Ofensas aos chamados direitos de personalidade. Manutenção da indenização. Provedor de internet. Serviço disponibilizado. Comprovação de zelo. Ausência de responsabilidade pelo conteúdo. Ação. Retirada da página em tempo hábil. Preliminar afastada. Denúncia da lide. Ausência de elementos. O dano deve representar ofensa aos chamados direitos de personalidade, como à imagem e à honra, de modo a desestabilizar psicologicamente o ofendido. V. A prática de *Bullying* é ato ilícito, haja vista compreender a intenção de desestabilizar psicologicamente o ofendido, o qual resulta em abalo acima do razoável, respondendo o ofensor pela prática ilegal. VI. Aos pais incumbe o dever de guarda, orientação e zelo pelos filhos menores de idade, respondendo civilmente pelos ilícitos praticados, uma vez ser inerente ao pátrio poder, conforme inteligência do art. 932, do Código Civil. Hipótese em que o filho menor criou página na internet com a finalidade de ofender colega de classe, atrelando fatos e imagens de caráter exclusivamente pejorativo. VII. Incontroversa ofensa aos chamados direitos de personalidade do autor, como à imagem e à honra, restando, ao responsável, o dever de indenizar o ofendido pelo dano moral causado, o qual, no caso, tem natureza *in re ipsa*. VIII. *Quantum* reparatório serve de meio coercitivo/educativo ao ofensor, de modo a desestimular práticas reiteradas de ilícitos civis. Manutenção do valor reparatório é medida que se impõe, porquanto harmônico com caráter punitivo/pedagógico comumente adotado pela Câmara em situações análogas. Apelos desprovidos" (TJRS, Apelação Cível 70031750094, 6ª Câm. Civ., rel. Liege Puricelli Pires, j. 30-6-2010).

"Ação de indenização. Dano moral. Ofensas e acusações em *sítio* de relacionamentos. Orkut. Prova nos autos que demonstra que a ré se utilizou do *sítio* de relacionamentos Orkut para ofender, proferir acusações e denegrir a imagem da autora, perante todas as pessoas que têm acesso ao conteúdo das mensagens de cunho manifestamente ofensivo. Violação a direito de personalidade, de molde a atingir a honra e imagem da parte autora. Danos morais configurados. Redução do *quantum* indenizatório. Sentença parcialmente reformada. Recurso parcialmente provido" (TJRS, Recurso Cível 71002312858, rel. Eduardo Kraemer, j. 26-3-2010).

mundo real, que dirá no mundo virtual. O ideal é a análise caso a caso, considerando que a legislação existente é perfeitamente aplicável, sobretudo se a Internet for entendida como um veículo de comunicação e mídia.

Neste sentido, cite-se como exemplo a decisão do Tribunal de Justiça de Goiás, de 16-1-2007, nos autos do processo n. 200300032595, que condenou renomado banco ao pagamento de danos morais a um cliente que, em razão de fraude praticada por terceiro na Internet, teve valores retirados de sua conta corrente, de modo que, em razão desse fato, teve cheques devolvidos e, consequentemente, o seu nome inscrito em órgãos de proteção ao crédito. A decisão frisou o fato de que, a despeito da instituição financeira ter ressarcido os danos materiais sofridos pelo cliente, deveria o banco responder objetivamente, também, pelos danos morais, uma vez que, no caso em tela, teria havido falha na prestação do serviço colocado à disposição do cliente (no caso, serviço de "internet banking").

Outra decisão interessante sobre danos morais e Internet se deu na 3ª Turma Recursal Cível dos Juizados Especiais Cíveis do Estado do Rio Grande do Sul, nos autos do Processo n. 71001272723. Em breve resumo, um sujeito houvera cobrado de outro dívida anteriormente contraída através do *sítio* de relacionamentos "Orkut" e, em razão desse fato, o devedor, sentindo-se ofendido, ajuizou ação de danos morais em face daquele, a qual foi julgada procedente pela Turma Recursal, uma vez que "ante o flagrante conteúdo depreciativo do recado" e, consequentemente, dano à imagem do autor, até pelo universo considerável de usuários do *sítio*, fazia-se justa tal condenação.

No ambiente digital, talvez o mais difícil de definir seja o momento exato no qual uma "não conduta", um "não agir", gera uma omissão passível de penalidade por negligência. Ou seja, quanto tempo da solicitação de remoção do ar de um determinado conteúdo poderia se considerar que a parte que tem meios técnicos para tanto está sendo relapsa ou mesmo conivente com a situação?

Conforme pesquisa realizada em conjunto com o advogado Dr. Vinicius Garcia, verificamos que não chega a haver um padrão de tempo limite para a remoção de conteúdo definido nas decisões judiciais brasileiras para retirada de conteúdo da internet, até pelo tema ser recente.

No entanto, pela amostragem analisada, há de se considerar uma tendência, observada pela determinação de cumprimento das decisões de forma imediata ou entre 24 e 72 horas, sendo que, em grande parte dos casos, tais deliberações costumam ser cumpridas dentro do prazo estabelecido. Isso se deve ao fato de que deve ser aplicada a legislação que determina ação imedia-

ta de intermediários objetivando a interrupção de ato lesivo perpetrado por terceiros, buscando o resultado prático equivalente. Isso está descrito no art. 461, § 5º, do Código Civil, no art. 84 do Código de Defesa do Consumidor e nos arts. 12, 19, 20 e 21 do Código Civil.

Considerando os provedores de serviço e de hospedagem como “meio” para violação a direitos no meio digital, e tendo em vista a responsabilidade por culpa (especialmente a omissão ou negligência a partir da ciência da publicação do conteúdo que muitas vezes contraria seu próprio termo de uso ou política), ou mesmo ainda a responsabilidade pelo risco do próprio negócio, não se pode deixar de lado sua fundamental importância na obtenção de resultado prático equivalente, frente à dificuldade de identificação, à primeira vista, dos responsáveis diretos pelos ilícitos cometidos.

Ou seja, o provedor não pode ser responsabilizado pela publicação em si, pois não há censura prévia, mas por deter os recursos técnicos que permitem sua remoção, quando muitas vezes inclusive é impossível identificar o autor até pela condição de anonimato permitida pelas suas próprias ferramentas. Se ficar inerte, mesmo frente a um pedido formal (escrito), por certo se torna responsável pela omissão e até mesmo conivente e cúmplice da lesão.

Como pudemos observar, então, os provedores de serviços na internet, têm, sem sombra de dúvida, capacidade técnica para implementar formas de controle e contingência, possibilitando a preservação de direitos e a cessação da sua violação quando determinado judicialmente.

Desse modo, pela análise da jurisprudência pátria, consideradas as peculiaridades casuísticas, a determinação de retirada de conteúdo da internet pelos provedores de forma imediata ou com prazos de 24, 48 ou 72 horas, atende ao princípio da razoabilidade¹¹.

11. Decisões judiciais recentes sobre o tema do prazo de retirada do ar de conteúdo na internet e outras notícias:

“2012 — STJ fixa prazo para retirada de mensagens em redes sociais como Orkut e Facebook; Google deve entrar com recurso — por Júlia Borba, de Brasília. O Superior Tribunal de Justiça determinou que mensagens publicadas em redes sociais, como Orkut e Facebook, que sejam consideradas ofensivas ou impróprias pelos usuários terão de ser retiradas do ar em até 24 horas após serem denunciadas. Empresas responsáveis por serviços de e-mail, como Hotmail e Google, serão obrigadas a fornecer auxílio na localização do remetente de mensagens que causem danos morais. As decisões foram tomadas pela ministra Nancy Andrighi. A primeira, que trata sobre redes sociais, foi provocada por uma carioca que se divorciou. Pouco tempo depois ela descobriu um perfil falso em seu nome no Orkut. A mulher apontou o conteúdo como ilícito, mas a suspensão da página ocorreu só dois meses depois. A Justiça determinou que o Google pague R\$ 10 mil a ela. Também decidiu que a empresa, dona do Orkut, fica obrigada a suspen-

No que tange à abordagem internacional sobre o tema, em 10 de fevereiro de 2003, a *Europe's Information Society* publicou os “Princípios de Segurança para Redes Sociais na União Europeia”. Citado documento estabeleceu que os provedores de redes sociais analisados compartilhavam de objetivo comum,

der conteúdos denunciados dentro de um dia, sem apuração prévia. Depois dessa medida, a empresa deverá checar se o caso é verdadeiro e se mantém a suspensão. ‘A decisão abre precedente no STJ e uniformiza a jurisprudência. É um marco de regulamentação e todas as futuras questões estarão sob essa ótica’, disse Andrighi. Se a empresa não cumprir o prazo, ela passará a ser responsável solidária pelo dano, podendo ser acionada na Justiça. ‘Fiquei sabendo que nos EUA eles são capazes de tirar as mensagens em 30 minutos. Levar 62 dias no Brasil é um absurdo’, disse Andrighi”, (*Folha de S.Paulo*, disponível em: <http://www1.folha.uol.com.br/fsp/mercado/50220-post-ofensivo-tera-de-sair-do-ar-em-24-horas.shtml>).

“STJ contribui para criar jurisprudência no mundo digital”, notícia de 20-3-2011, disponível em: http://www.stj.gov.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=101146. “(...) Em contraponto, a ministra Nancy Andrighi afirma que, mesmo que fosse possível vigiar a conduta dos usuários sem descaracterizar o serviço prestado pelo provedor, haveria de se considerar outro problema: os critérios que autorizariam o veto ou o descarte de determinada informação. Seria impossível delimitar parâmetros de que pudessem se valer os provedores para definir se uma mensagem ou imagem é potencialmente ofensiva. ‘Entretanto, também não é razoável deixar a sociedade desamparada frente à prática, cada vez mais corriqueira, de se utilizar comunidades virtuais como artifício para a consecução de atividades ilegais’, declara. Ao negar provimento ao recurso, a ministra destacou que os provedores de conteúdo não respondem objetivamente pela inserção no site, por terceiros, de informações ilegais e que eles não podem ser obrigados a exercer um controle prévio do conteúdo das informações postadas no site por seus usuários. Mas, devem assim que tiverem conhecimento inequívoco da existência de dados ilegais no site, removê-los imediatamente, sob pena de responderem pelos danos respectivos, mantendo, dessa forma, um sistema minimamente eficaz de identificação de seus usuários. (...)”.

Outros: “Redes sociais são mais ágeis que SAC como canal de reclamação”, *Folha de São Paulo*, 13-10-2011, disponível em: <http://www1.folha.uol.com.br/tec/989698-redes-sociais-sao-mais-ageis-que-sac-como-canal-de-reclamacao.shtml>; “Social Media Users Expect Rapid Live Help, According to Consumer Report from Oracle Study Shows Consumers Prefer to Reach Customer Service Online”, *Oracle Press Release*, 14-5-2012, disponível em: <http://www.oracle.com/us/corporate/press/1627424>; “Parecer defende responsabilidade do Google por manter conteúdo abusivo no Orkut”, *Notícias Procuradoria Geral da República*, 12-6-2012, disponível em: http://noticias.pgr.mpf.gov.br/noticias/noticias-do-site/copy_of_geral/parecer-defende-responsabilidade-do-google-por-manter-conteudo-abusivo-e-foto-publicada-sem-autorizacao-no-orkut; “Relatório com a quantidade de pedidos para remover conteúdo dos resultados de pesquisa no buscador da empresa”, *Google Transparency Report*, disponível em: <http://www.google.com/transparencyreport/removals/government/>; “Google agrees to court order in India to remove content”, *PC World Australia*, disponível em: http://www.pcworld.idg.com.au/article/414468/google-agrees-court_order_india_remove_content/; “Facebook and Google remove ‘offensive’ India content”, *BBC News India*, disponível em: <http://www.bbc.co.uk/news/world-asia-india-16903765>; “Google, Facebook get 15 days deadline to remove ‘objectionable’ content”, *The Times of India*, disponível em: http://articles.timesofindia.india-times.com/2012-02-06/internet/31029861_1_anti-religious-or-anti-social-content-facebook-and-google-delhi-court; “EU withdraws ‘racist’ video clip” (The European Commission has withdrawn a video promoting EU enlargement after it was accused of being racist), *BBC News Europe*, disponível em: <http://www.bbc.co.uk/news/world-europe-17276838>.

qual seja, maximizar os benefícios da internet e gerenciar os riscos inerentes ao meio.

Em suas intenções, o documento citado deixa claro que as empresas/provedores devem desenvolver continuamente estratégias de segurança e boas práticas, estabelecendo princípios para minimizar danos, contudo, sem caráter vinculativo. Dentre os princípios enumerados, destacam-se:

- *Principle 4: Provide easy to use mechanisms to report conduct or content that violates the Terms of Service* (fornecer mecanismos de fácil acesso para relatar conduta ou conteúdo que viole os Termos de Serviço) e;

- *Principle 5: Respond to notifications of Illegal content or conduct* (resposta a notificações de conteúdo ou conduta ilegal).

Segundo entendimento adotado pela União Europeia, os provedores devem fornecer mecanismos para denúncia de conteúdos inadequados, sendo que tais comportamentos devem estar descritos nos “Termos de Uso” de cada serviço.

O *Principle 5* ainda prescreve que, recebida uma notificação de abuso de direito, devem os provedores *rapidamente* rever e, se necessário, *remover* conteúdos que violem direitos e os Termos de Uso. Interessante observar que tal princípio estabelece a possibilidade de existência de “canais de emergência”, como, por exemplo, os contatos 999 (UK) ou 112 (EU).

Orientada pelos princípios acima descritos, a *Europe's Information Society*, em setembro de 2011, publicou os resultados de uma avaliação independente da aplicação dos princípios de redes sociais mais seguras na EU, feita em nove sites de redes sociais.

No período de março a junho de 2011, nove sites operados por sete dos signatários foram testados e os resultados foram publicados em setembro daquele ano: *Dailymotion*, *Flickr*, *Habbo Hotel*, *Stardoll*, *Skyrock*, *Windows Live*, *Yahoo Pulse*, *YouTube* e *Xbox Live*. No período de dezembro de 2010 a janeiro 2011, 14 websites mantidos por 14 dos signatários foram testados e os resultados foram publicados em junho de 2011: *Arto*, *Bebo*, *Facebook*, *Giovani.it*, *Hyves*, *MySpace*, *Nasza-klaza.pl*, *Netlog*, *Um.lt*, *Ratee*, *SchülerVZ*, *IRC Galleria (Sulake)*, *Tuenti* e *Zap.lu*.

Entre um dos itens analisados podemos destacar a análise: “*Principle 4 — Easy To Use Mechanisms For Reporting Violations*”. No referido item, pode-se verificar que, dos oito serviços analisados, sete responderam às solicitações de

usuários com alguma ação, como restringir ou excluir conteúdo. Em alguns casos, foram emitidos pelos provedores avisos aos usuários que tinham violado os Termos de Uso ou orientação para que as partes resolvessem o conflito entre si.

Frise-se que, na maior parte dos casos analisados, as notificações foram respondidas dentro de 24 horas, sendo que, em um dos casos, a resposta para a notificação foi enviada no prazo de 24 horas, mas o conteúdo reportado foi removido somente após 48 horas.

Como resultado das notificações, na maior parte dos casos, o conteúdo foi permanentemente removido ou ocorreu alguma restrição decorrente de conteúdo inapropriado em função de menoridade, sendo que em apenas um caso foi tomada medida contra o usuário.

Diante do exposto, pode-se verificar clara possibilidade técnica de análise e reposta às notificações de abuso feitas pelos usuários dentro do prazo de 24 horas.

Destacamos ao final a importância de se utilizar esse tipo de mecanismo de retirada de conteúdo do ar sem ordem judicial de forma cautelosa, pois, independentemente do benefício da maior proteção da vítima da ofensa, considerando o princípio da liberdade de expressão, que se coaduna também com o da ampla defesa, devemos fazer uma ressalva de que toda e qualquer remoção de conteúdo deva ser devidamente documentada com a denúncia formal realizada ao provedor, até para evitar que haja arbitrariedade e que a justificativa de suspensão e remoção de conteúdo acabe sendo distorcida e utilizada com finalidade de cercear a livre manifestação do pensamento, com intuito inclusive político. Deve haver uma exigência de que seja garantido o devido processo legal, para que também uma denúncia infundada faça com que a vítima de censura também encontre guarida do Judiciário.

Pelo princípio do menor dano, é melhor remover do que manter no ar, mas, sendo infundada a denúncia, deve-se garantir a volta ao ar do conteúdo e também a punição daquele que tenha sido leviano, visto que aí a lesão será à liberdade, em vez de à privacidade (como vem ocorrendo mais comumente, em geral, ferindo a honra e a reputação).

Sendo assim, como vimos, a legislação vigente no tocante à responsabilidade civil é totalmente aplicável à matéria digital, devendo apenas observar as particularidades do meio virtual ou dos demais meios convergentes, como já ressaltamos.

“Educar em uma sociedade da informação significa muito mais que treinar as pessoas para o uso das tecnologias de informação e comunicação: trata-se de investir na criação de competências suficientemente amplas que lhes permitam ter uma atuação efetiva na produção de bens e serviços, tomar decisões fundamentadas no conhecimento, operar com fluência os novos meios e ferramentas em seu trabalho, bem como aplicar criativamente as novas mídias, seja em uso simples e rotineiros, seja em aplicações mais sofisticadas. Trata-se também de formar os indivíduos para ‘aprender a aprender’, de modo a serem capazes de lidar positivamente com a contínua e acelerada transformação da base tecnológica.”

“A atração que as novas tecnologias exercem sobre todos — de formuladores de políticas e implementadores de infraestrutura e aplicações de tecnologias de informação e comunicação até usuários de todas as classes e idades — pode levar a uma visão perigosamente reducionista acerca do papel da educação na sociedade da informação, enfatizando a capacitação tecnológica em detrimento de aspectos mais relevantes.”

TAKAHASHI, Tadao (Org.). *Sociedade da informação no Brasil: livro verde*. Brasília: Ministério da Ciência e Tecnologia, 2000, p. 45.

Com o atual cenário de uma sociedade cada vez mais digital não há como se esquivar da necessidade de educar e orientar os jovens quanto às condutas também no ambiente virtual. Não basta apenas entregar, disponibilizar uma máquina para o aluno e ensiná-lo a utilizar suas diversas funções se não aprenderem também que devemos zelar pela segurança digital bem como agir de forma ética e legal a fim de sermos bons cidadãos digitais.

Acreditamos, portanto, que a educação digital deve ser promovida simultaneamente à inclusão digital dos usuários, seja dos indivíduos que estão tendo o primeiro contato com as máquinas somente no ambiente de trabalho, seja da nova geração que já nasceu dentro de uma sociedade totalmente informatizada. Este último grupo necessita de orientação especial, já que crianças e adolescentes estão passando pelo amadurecimento de seus conceitos éticos, morais e de cidadania.

É extremamente necessário que pais e escolas invistam na educação digital de seus filhos. Já não basta apenas orientá-los a não abrir a porta de casa para estranhos. Eles precisam saber também que não é seguro abrir *e-mails* de estranhos. Esse tipo de ensinamento deve ser aplicado em atividades lúdicas e escolares para, no futuro, ser adotado também no ambiente profissional.

Da mesma forma que escolas utilizam cartilhas com o bê-á-bá, também devem ser adotados materiais que prendam a atenção do aluno e transmitam mensagens de segurança da informação, boas práticas digitais e de ética, sendo, portanto, de grande valor a existência de aulas sobre Cidadania e Ética Digital¹ nos cursos que envolvem uso de computador para os alunos.

A formação precoce do cidadão digital é de vital importância para a segurança e o bom uso dos meios eletrônicos disponíveis. Começar desde cedo é fazer um investimento seguro e altamente rentável no futuro de nossos profissionais.

Para que seja desenvolvida uma consistente base de conhecimento digital nos jovens, cartilhas, vídeos, palestras e *games* podem ser desenvolvidos como forma de alcançar tal objetivo². Como é característico dessa faixa etária, os projetos são dinâmicos, interativos, didáticos e com alto grau de retenção de conhecimento. Dado que existe alto interesse pelo assunto, há uma interação muito rica entre o grupo, resultando em diversas perguntas, até mesmo dias

1. Atualmente, vários procedimentos de conduta estão sendo divulgados pela mídia como forma de educar o cidadão no correto uso dos benefícios trazidos pela informática. Como exemplo, podemos destacar o Código de Ética Anti-spam, apresentado pelo Comitê Brasileiro Anti-spam (<http://www.brasilantispam.com.br/>), o qual tem por objetivo reger e orientar a comunicação institucional, comercial e publicitária enviada sob a forma de mensagens eletrônicas, sem prejuízo da concomitante aplicação, quando for o caso, da legislação vigente, especialmente em matéria de publicidade, privacidade e proteção ao consumidor.

2. Como referência pioneira no assunto, destacamos o *Manual do motorista virtual*, que corresponde a uma ferramenta de educação digital, no qual o usuário “dirige” por um cenário que explica conceitos de Certo e Errado no uso da tecnologia, comparando o uso do computador com o carro. O material é ideal para campanhas de conscientização de segurança da informação na empresa e também pode ser adaptado para escolas e centros de capacitação profissional. Para saber mais, acesse os links <<http://www.brochura.com.br/elearning/>> ou <<http://www.brochura.com.br/manual/>>, bem como o site <<http://www.patriciapeck.com.br/>>.

após os treinamentos. É estabelecido um canal permanente de contato para que nenhum aluno fique com dúvida sobre o assunto.

Educar na sociedade digital não é apenas ensinar como usar os aparatos tecnológicos ou fazer efetivo uso da tecnologia no ambiente escolar. Educar é preparar indivíduos adaptáveis e criativos com habilidades que lhes permitam lidar facilmente com a rapidez na fluência de informações e transformações. É preparar cidadãos digitais éticos para um novo mercado de trabalho cujas exigências tendem a ser maiores que as atuais.

Para aplicar este princípio de educação, o professor deve antes de qualquer coisa entender que os jovens de hoje em dia são diferentes do que fomos quando na idade deles. Nasceram em uma era analógica bem diferente da era digital atual, em que a lógica de raciocínio e atenção múltipla é uma constante. Os professores devem esforçar-se em conhecer o mundo no qual os jovens vivem hoje e passar a enxergar a realidade da perspectiva deles, ou acabarão assumindo a posição de alienígenas em sala de aula. Essa divisão de realidades e isolamento do professor dificultará a cumplicidade entre ambos e, consequentemente, a eficácia do ensino.

O educador deve sempre atualizar-se e ficar atento ao mundo deste novo aluno. Deve procurar conhecer os programas digitais que mais o interessa e descobrir o que motiva esse interesse no aluno, bem como buscar formas que possibilitem sua utilização em benefício do aprendizado. Não adianta passar um monte de tarefas para serem feitas após a aula, quando a realidade do estudante é diferente. Hoje, o estudante sai da escola, vai para casa e faz tudo ao mesmo tempo: assiste à televisão, navega na Internet e faz a tarefa. O professor deve tornar as atividades interessantes para conquistar o interesse e a atenção do aluno. É um desafio, mas o contato com o mundo em que o jovem vive atualmente facilitará ao professor aplicar sua criatividade em atividades que incentivem o aluno. Já não há como voltar no tempo; a tecnologia veio para ficar e o educador tem o dever de se adaptar e criar novas formas de ensino.

A Internet não será extinta e novas tecnologias ainda estão a surgir. Com o passar do tempo, muito mais pessoas estarão conectadas à rede mundial, e negar tal fato é como negar a própria evolução da sociedade. Nesse sentido:

“No meio dos anos 90 do século XX, quando pensadores de áreas distintas haviam percebido que a sociedade entrara em um novo padrão de poder e referência, um escritor brasileiro, a pretexto de fazer uma crítica à pós-modernidade — o delírio a favor estava se esgotando e os novos profetas pareciam dizer: eu te disse, eu te disse, eu te disse —, pregava que qualquer mudança só seria possível quando partíssemos da possibilidade de extinção da televisão. Isso mesmo: extinção da televisão.

(...)

*Ninguém desligará a televisão. Ao contrário. Ela cresce de importância e se diversifica. Mais e mais gente acessará a Internet — é um fato. A ciência e a tecnologia continuarão a gerar, aqui e ali, experimentos e resultados dirigidos às expectativas investidas. E ambas — ciência e tecnologia — talvez sejam geridas por regras internacionais, como, aliás, já existem atualmente. Assim, deste ponto no tempo onde estamos, é difícil dizer o que virá. Mas sempre, até o momento, os acontecimentos vieram para melhor*³.

É crescente o incentivo e a utilização das ferramentas tecnológicas como apoio pedagógico, cada vez mais professores buscam apoio nos *blogs* e comunidades. Projetos de inclusão digital surgem a cada dia.

Deparamo-nos, portanto, com situações inéditas e inesperadas. Prova disso é o surgimento de uma nova linguagem usada na comunicação *online*, em que abreviações são constantes em diálogos digitais, de forma a acompanhar a velocidade da sociedade da informação. Não adianta lutar contra um costume digital que tem sido mundialmente adotado. Não defendemos a adoção de uma nova linguagem, mas também não podemos negá-la. O papel da escola está em orientar o aluno sobre as ocasiões em que esta linguagem informal pode ser usada e as que exigem formalidade. Diante dessas mudanças, devemos nos adaptar!

Nesta nova sociedade digital, o advento da Internet traz maravilhas que o professor deve tomar como vantagens. Educadores devem compreender que o maior risco que as crianças e adolescentes correm é não terem acesso à Internet. A rede é essencial na educação dos jovens, bem como na preparação de suas futuras carreiras profissionais.

A lista de benesses que a rede nos proporciona é infinita! Com ela os alunos têm a oportunidade de atravessar fronteiras, derrubar barreiras e dividir ideias de forma única. E um de nossos objetivos é trazer situações que contribuam para sua construção do conhecimento, preparando-os para a cidadania digital e para uma realidade diária mais segura.

O jovem também precisa aprender que cada um é responsável pelo que escreve e que deve pensar várias vezes antes de publicar algo *online* porque os resultados de um conteúdo mal colocado podem ser avassaladores. O usuário pode ser punido tanto no âmbito administrativo/escolar quanto no Judiciário,

nos casos mais graves. O problema está na falta de conhecimento e habilidades nas crianças e na maioria dos jovens para reconhecer os perigos *online*. É preciso orientá-los nesse sentido para que possam desenvolvê-las e aplicá-las por si.

Devem eles ter em mente que os seus atos no ambiente virtual geram consequências na vida real. A Internet, como muitos acham, não é território de ninguém.

É inevitável, sem dúvida, que os jovens no ambiente de Internet se deparem com pornografia, com *sites* que promovem a delinquência (destruir, construir armas, falsificar documentos, piratear programas e documentos etc.), *sites* que promovem o suicídio, a bulimia e a anorexia, *sites* de jogos, entre outros. Entretanto, suas atitudes diante de situações como essas é que farão toda a diferença!

Conforme exposto anteriormente, a tecnologia veio para ficar: celulares são computadores, televisores são interativos, Internet também é telefone e celulares transmitem programação televisiva, só para citar alguns. Acompanhem os números, pesquisas e estatísticas, segundo o *IDGNow*, disponível em <www.idgnow.com.br/indices>.

Assim, concluímos o fim de uma era analógica sob a qual fomos criados e educados, para agora termos o desafio de adaptação, inclusão e educação na era digital. Para preparar os trabalhadores de amanhã para esta era, precisamos modificar nosso ponto de referência e visão por meio de nossa própria educação.

3. RESENDE, André. *Mundo enquadrado: o lugar dos símbolos nas coisas reais*. São Paulo: Altana, 2005. p. 12 e 15.

Os Principais Tipos de Usuários de Tecnologia e seus Impactos no Direito

A grande maioria dos incidentes relacionados ao uso de ferramentas tecnológicas e informações nas empresas é provocada pelo usuário “sem noção”, e apenas 2% envolvem usuários de “má-fé”. Ou seja, a negligência no uso seguro das ferramentas, a falta de conhecimento das regras, melhores práticas e leis vigentes no Brasil provocam consequências desastrosas e em tempo real para muitos profissionais. Por isso, vamos aprender a ser um usuário mais consciente, digitalmente correto e dar o exemplo não apenas no trabalho, mas em casa e na família, já que muitos têm a missão de ensinar também seus filhos, que são a próxima geração da força de trabalho, para construir um Brasil sustentável¹!

Perfil 1.0 — “*homo analogicus*”: este perfil tem fobia a tecnologia. Aprendeu tudo na era do papel, do mundo mais físico e presencial. É da era do “cata milho” e da máquina de escrever. Em geral, tem dificuldade em usar ferramentas tecnológicas, não gosta de ter senha, não confia nas máquinas. Por isso,

1.

Manual de Sobrevivência Digital	
• Evite passar senhas para terceiros (mesmo que da família ou conhecidos). Se o fizer, mude em seguida. Sempre ao sinal de suspeita que alguém saiba a sua senha, a altere.	• Busque sempre estar com antivírus e <i>antispyware</i> atualizado, bem como faça uso de <i>firewall</i> e demais <i>softwares</i> de segurança, inclusive para criptografia das informações, para <i>backup</i> , há muitas opções boas e baratas e algumas também gratuitas. O importante é não ficar sem.

costuma passar a senha para outra pessoa realizar a tarefa, seja secretária, filho, colega. É um alvo fácil para engenharia social.

Perfil 2.0 — “homo semidigitalis”: este perfil está em transição. Cresceu na era mais analógica, com pais analógicos, avós analógicos e foi forçado a se digitalizar por causa da necessidade de trabalho (usar computador, ter senha, ter *e-mail*, ter celular, navegar na Internet). Para ele, tecnologia é uma obrigação, um mal necessário. Já ousa pesquisar preço na Internet, mas prefere imprimir a oferta e ir até a loja física para levar o produto debaixo do braço por garantia. Não costuma baixar conteúdos, mas aprendeu a colocar a foto dos filhos no fundo de tela do computador e do celular. É comum já ter computador em casa e assinar banda larga, mas para uso da família, ele mesmo não usa. Este perfil ainda é sem malícia, sujeito a ser usado como um “laranja digital”.

Perfil 3.0 — “homo digitalis”: este perfil ocorre em geral com aqueles que ganharam um “videogame” quando eram pequenos ou tiveram acesso à tecno-

• Evite deixar o computador ligado e logado quando estiver ausente. Sempre faça bloqueio de tela ou se for se ausentar por longo período é recomendável desligar o equipamento e tirar da tomada.	• Busque usar apenas equipamentos que estejam com <i>softwares</i> de segurança atualizados, especialmente se for em local público, cybercafé, <i>lanhouse</i>, rede de hotel. Na dúvida pergunte para o responsável do serviço. Se possível, evite colocar sua senha de transações (bancária e cartão de crédito) nestes equipamentos. Ao encerrar a sessão, certifique-se que apagou tudo da máquina e fez <i>logout</i> de todos os ambientes.
• Insira senha em celular, para bloqueio automático por inatividade. Também deve-se fazer <i>backup</i> da agenda, apagar periodicamente mensagens e <i>e-mails</i> do dispositivo (se possível uma vez por semana) para evitar as suas informações pessoais e sigilosas caíam em mãos erradas.	• Evite fazer uso de fotos (imagens) de pessoas (especialmente crianças) que você não tenha autorização prévia, escrita para tanto. Na dúvida, se a pessoa vai gostar ou achar ruim, é melhor não usar. Principalmente se você tiver encontrado em um <i>site</i> de fotos/imagens cuja origem das fotos é desconhecida.
• Evite carregar equipamentos tecnológicos que chamem a atenção quando estiver caminhando, andando de carro ou de táxi, especialmente <i>notebook</i>, celular, MP3. Seja discreto e cuidadoso, se possível coloque na mala do carro e em uma mochila.	• Sempre leia tudo que lhe for apresentado para dar <i>click-ok</i> na Internet. Mesmo que você não possa mudar nada, deve-se sempre saber com o que se está concordando. Termos de uso, políticas de privacidade, avisos legais de direitos autorais, licenças, garantias, comprovante compra-e-venda <i>online</i>, tudo isso é documento, é prova legal. “Não assine sem ler, especialmente na web”.
• Evite deixar seus pertences tecnológicos soltos, em cima da mesa de estudo, de trabalho, em uma cadeira no restaurante para se servir (especialmente quando é <i>buffer</i> ou quilo, ou restaurante de hotel no horário de café da manhã que tem maior incidência de furtos). Fique de olho sempre.	• Seja cauteloso para quem você passará seus dados na Internet. Selecione bem, certifique-se. Lembre-se de que na era da informação não existe almoço grátis. Todo serviço gratuito tem como preço a sua informação. Assim como ofertas mirabolantes podem significar um golpe de loja fantasma digital, tenha cuidado com <i>e-mails</i> que possam ser falsos, não clique em tudo que recebe por <i>e-mail</i> ou vê na Internet. Na dúvida, acesse direto o <i>site</i> ou entre em contato pelo SAC <i>online</i>.
• Evite ofender pessoas ou empresas na Internet. Use uma linguagem apropriada, que não seja agressiva, pois se deve exercer a liberdade de expressão com responsabilidade. Aquele que abusa do direito, também comete ilícito e está sujeito a indenizar o outro lesado.	• Não faça justiça com o próprio <i>mouse</i>. Se algo de ruim lhe acontecer no uso de tecnologias, na Internet, denuncie, busque ajuda de um especialista, comunique a autoridade. Preserve as provas digitais, evite mexer novamente na máquina. Se não for sua, peça ao proprietário que a reserve para coleta das provas.

logia ainda na escola ou na faculdade. Sua principal característica é ter aprendido a usar computador primeiro por motivo de lazer. É bem mais multimídia. Prefere imagens e áudio a textos. Este usuário participa de redes sociais em geral, gosta de ouvir MP3, baixar várias coisas na Internet (principalmente se for de graça) e tem uma leve tendência a fazer “cópia e cola” do conteúdo alheio, sem achar que está fazendo nada errado. Assim que recebe sua máquina na empresa, já tenta mudar o fundo de tela, personalizar. Este perfil costuma achar ruim qualquer proibição. Já sabe usar bastante os recursos, mas não tem o hábito de segurança, costuma deixar a máquina aberta, usar maciçamente cybercafé ou *lanhouse*. É conhecido como “sem noção”, faz tudo sem saber que risco corre, qual a consequência dos seus atos e que danos pode sofrer ou gerar para os outros.

Perfil 4.0 — “homo digitalis-mobilis”: este perfil é a versão 3.0 evoluído com mobilidade, já com uma necessidade de usar tecnologia independente de onde estiver, ou seja, sua relação de tempo-espço já foi transformada. Para ele, *desktop* é pré-histórico. É pela mobilidade total. Tudo tem de ser pequeno, portátil, para exercer ao máximo seu direito de ir e vir. Se pudesse não ia para o trabalho, fazia tudo sem sair de casa, afinal, na era da VPN, do *notebook*, do *smartphone*, do VOIP, da educação a distância e da *webconference* para quê sair de casa? Sofre com o excesso de exposição que passou a ter na *web*. Já vive plenamente a era dos dados, é tudo por escrito. Não foi educado nas leis, acha que as mesmas não se aplicam para a Internet, para ele “os fins justificam os *e-mails*”. É um “sem noção” que costuma “fazer justiça com o próprio *mouse*”.

Perfil 5.0 — “homo tecnologicis seguro”: este é o usuário evoluído, digitalmente correto, com comportamento ético, seguro e legal no uso das tecnologias. Não importa sua idade, ele foi ensinado e criou o hábito da segurança da informação. Sempre se preocupa em fazer do jeito certo, em estar seguro. Faz sempre *back-up*, tem plano de contingência pessoal para não ficar sem seus dados. Já aplica o Manual de Sobrevivência Digital (abaixo). Não acredita em tudo que vê na Internet. É mais preocupado em preservar sua reputação digital, por isso mede muito bem as palavras escritas que vai publicar ou enviar por *e-mail* ou SMS. Está sempre buscando novas formas de se proteger. Sabe guardar as provas eletrônicas, sabe fazer denúncia na Delegacia de Crimes Eletrônicos e está preparado para os novos desafios da sociedade digital.

Por este motivo, educação é fundamental. Formar o usuário digitalmente correto! Motivo este que originou o movimento “Criança Mais Segura na Internet”², que é uma iniciativa de responsabilidade social digital, na área edu-

2. Disponível em: <www.criancamaisseguranainternet.com.br>.

cacional, idealizada pelo escritório e abraçada pela Associação Brasileira de Anunciantes (ABA), com diversas grandes empresas copatrocinadoras, que busca conscientizar pais e filhos sobre o uso ético, seguro e legal das tecnologias, bem como formar e capacitar professores e voluntários para ministrar palestras e aulas do tema. Foram produzidos diversos materiais didáticos que estão disponíveis de modo gratuito no *site*, as escolas podem solicitar uma palestra gratuita do Movimento, tem cartilha e filmes que ilustram esta vida digital, o dia a dia dos jovens que cada vez mais cedo passam a fazer o uso de Internet.

O Movimento tem como objetivo formar usuários digitalmente corretos para construir um Brasil sustentável na sociedade digital, o que só será possível com forte base em ética e legalidade. Por isso, há um abaixo-assinado digital com a proposta de apresentar um projeto ao MEC para incluir a disciplina de Cidadania e Ética Digital na grade dos ensinos fundamental e médio das escolas públicas e privadas. Quando isso ocorrer, já teremos professores capacitados, material didático e muito apoio da família. É o Direito Digital entrando na vida do indivíduo.

Primeiramente, em sua definição clássica, contrato é o acordo de vontades entre duas ou mais pessoas com a finalidade de adquirir, resguardar, modificar ou extinguir direito. Para o Direito Digital, os contratos têm algumas características peculiares que determinam a necessidade de aprofundar questões normalmente não aplicadas em contratos tradicionais.

O primeiro diferencial é a terminologia¹. É recomendável o emprego de um glossário inicial que estabeleça o significado dos termos técnicos empregados no contrato realizado pelas partes. Isso possibilita um menor grau de interpretação, diminuindo o risco de duplo sentido ou de má compreensão do que está sendo contratado. Esse quesito é fundamental nos contratos da era digital, não só porque nascem novos termos quase diariamente, mas também em razão do sentido peculiar dado a palavras que normalmente têm outro significado no mundo real.

O segundo ponto importante do Direito Comercial e Societário Digital é determinar objetivamente as responsabilidades das partes quanto à tecnologia, à segurança, ao conteúdo, ao produto, à entrega, ao banco de dados, às

1. Esta é uma tendência iniciada pela Uncitral, órgão da ONU, que, em sua lei-modelo para o comércio eletrônico, arrola um pequeno vocabulário de termos técnicos, explicando como deveriam ser entendidos dentro do projeto. Assim também procedeu a Ordem dos Advogados do Brasil quando elaborou seu anteprojeto de lei para o comércio eletrônico, fortemente influenciado pelo projeto proposto pela Uncitral.

informações publicadas ou tornadas públicas, à atualização e ao *upgrade*. Devem existir cláusulas específicas, delimitando e definindo o grau de responsabilidade por todas essas questões e, principalmente, sobre a proteção da relação com o consumidor final, uma vez que o Código de Defesa do Consumidor é totalmente aplicável dentro do Direito Digital e das relações de consumo virtual.

O terceiro ponto implica o cuidado que as partes devem tomar quanto ao tipo de informação veiculada *online*² e na definição da responsabilidade por sua veracidade e atualização, já que a Internet é uma mídia que praticamente torna eterna muitas mensagens na rede, sem que seus autores as apaguem. No entanto, em uma relação comercial, pode haver danos causados em virtude dessas informações perdidas e mensagens fantasmas.

O quarto ponto é a necessidade de incluir no contrato uma cláusula arbitral³, já que celeridade, *expertise*, especialidade e sigilo são essenciais na solução das questões de Direito Digital.

Atualmente os contratos eletrônicos apresentam-se sob duas formas distintas⁴, como contratos-tipo, em que todas as cláusulas são impostas por uma

2. Como já tivemos oportunidade de expor, são, por analogia, aplicáveis à mídia eletrônica as leis que regulam as outras mídias tradicionais, incluindo a Lei de Imprensa e a Lei do Audiovisual, mas não se limitando a elas.

3. Os juízos arbitrais possuem inúmeras vantagens diante do nosso "processualismo". Os árbitros têm maiores conhecimentos técnicos, mas muitas vezes é a rapidez com que se resolvem as questões o ponto mais atrativo desta via alternativa. Porém, é necessário estar atento a uma questão na hora de inserir a cláusula arbitral: se o contrato for de adesão para consumidor final, a mera inclusão desta no contrato não gera nenhum efeito, isso porque o Código de Defesa do Consumidor em seu art. 51, VII, a considera uma cláusula abusiva, portanto, nula de pleno direito. A solução nesses casos é oferecer sempre a cláusula apartada do contrato e não vincular a aceitação de um a outro.

4. Além da classificação proposta existe uma outra, segundo Robson Ferreira, que leva em consideração a interatividade entre os contraentes, podendo assim dividir os contratos eletrônicos em:

"Contratos Eletrônicos Intersistêmicos: aqueles em que a contratação é feita entre sistemas aplicativos pré-programados, sem qualquer ação humana. Frequentemente entre pessoas jurídicas, para relações comerciais de atacado."

Contratos Eletrônicos Interpessoais: o computador oferece meio de comunicação para o acordo de vontades das duas partes, necessariamente ocorre interação humana nos dois pólos da relação. Podem ser simultâneos (celebrados online), ou seja, quando as partes estão ao mesmo tempo conectadas na rede. Têm analogia com os contratos firmados por telefone, aplicando-se o art. 428, I. E podem ser não simultâneos, em que existe lapso temporal entre a declaração de vontade de uma parte e a recepção desta pela outra parte, em geral, via e-mail; nesse caso, equivalem à correspondência, aplicando-se os arts. 1.086 e 434, caput, do Código Civil."

Contratos Eletrônicos Interativos: resulta de uma relação de comunicação entre uma pessoa e um

parte à outra sem que se possam discutir cláusulas isoladamente; e como contratos específicos, nos quais a elaboração é feita caso a caso; dependendo do *status* dos contraentes ou do objeto do contrato, prevalece uma modalidade ou outra.

Contratos-tipo são aqueles elaborados por uma das partes e oferecido à outra, a quem cabe apenas aderir incondicionalmente, sem que haja possibilidade de discussão; assim são, por exemplo, os contratos de agências bancárias e a maioria dos contratos de revendedores para com seus consumidores, visto que está implícito nessa modalidade uma desigualdade quanto ao poder de barganha. Por isso mesmo deve-se ter cuidado redobrado na elaboração de cada uma de suas cláusulas, pois o Código de Defesa do Consumidor não admite a estipulação de cláusulas que podem revelar-se abusivas⁵.

Os contratos que regulam relações de serviços de tecnologia, tais como segurança, *hosting*, conexão, entre outros, devem ser elaborados caso a caso entre as partes, porém com certeza em todos os contratos devem constar: atribuição de responsabilidades, garantia de atualização da tecnologia e a cláusula de equilíbrio econômico-financeiro.

No caso de imagens e fotos de produtos, é muito importante que elas tragam informações sobre a data em que foram registradas, evitando problemas de potencial publicidade enganosa, caso o tempo entre a imagem ou foto e o tempo de compra sejam muito distantes entre si.

Independentemente de ser ou não um contrato de alguma forma vinculado à *web*, a própria sociedade digital, que vem delineando seus aspectos mais importantes como seus próprios mecanismos de mudanças dinâmicas, exige que hoje se insiram nos contratos cláusulas de equilíbrio econômico-financeiro. Na sociedade digital, acima de qualquer outra, as relações entre economias e mercados estabelecem interdependência em nível global, e crises locais nacionais muitas vezes podem gerar crises sistêmicas.

Daí a importância da cláusula que afasta a responsabilidade do devedor por prejuízos advindos de um desequilíbrio econômico-financeiro, notadamente porque é uma causa de força maior⁶, totalmente alheia às partes, que são impotentes ante as aludidas crises.

sistema previamente programado, é a forma mais usual de contratação utilizada pelo e-commerce, em que a manifestação de vontade se dá com o clique do mouse, aplicando-se o art. 112 do Código Civil."

5. Código de Defesa do Consumidor, arts. 51, 52 e 53.

6. Código Civil, art. 393: "O devedor não responde pelos prejuízos resultantes de caso fortuito ou força maior, se expressamente não se houver por eles responsabilizado" (casos de mora).

O profissional ao elaborar o contrato deve ter em mente que cláusulas como estas, que tratam minuciosamente das responsabilidades dos contraentes, ajudam a dirimir conflitos e até a evitar demandas judiciais, porque trazem para dentro da responsabilidade contratual questões que de outra forma teriam obrigatoriamente de ser objeto de decisão judicial, com a lentidão e demais problemas do Poder Judiciário, que são incompatíveis com as necessidades da nova sociedade digital.

É aconselhável que seja observada também a necessidade ou não de ter uma cláusula de seguro, determinando o valor do prêmio e de quem é a obrigação de pagamento — se das partes ou se será embutido no preço final da mercadoria. Isso porque é uma das soluções mais eficientes para que todo o prejuízo ou dano causado devido à instabilidade do mercado digital quanto à segurança e aos padrões seja ressarcido, evitando que se tenha uma falta de credibilidade no meio enquanto via comercial e de realização de negócios.

Contratos que regem operações dentro do mundo virtual têm algumas peculiaridades que devem ser especialmente observadas: a) indicação clara das responsabilidades de todos os participantes da cadeia de relações envolvida, principalmente porque a Internet privilegia as relações em rede, com vários coparticipantes e especial atenção nos direitos do consumidor final; b) estabelecer uma política de informação clara; c) política de segurança e privacidade; d) cláusula de arbitragem; e) territorialidade⁷, estabelecendo os limites geográficos de ação de cada envolvido; f) relação dos parceiros envolvidos no negócio; g) no caso de os produtos transacionados envolverem tecnologia, estabelecer as responsabilidades por *upgrades* e obsolescência.

Uma das questões que mais se discutem em matéria de contratos virtuais é a da força probante dos contratos eletrônicos. No Brasil, ainda inexistem regras jurídicas específicas a respeito dessa questão, mas também não há nada que impeça a admissibilidade do documento eletrônico como meio de prova⁸.

7. As partes na maioria das vezes podem dispor sobre o foro competente para julgar lides com origem em determinado contrato, fixando assim o juízo competente. Ainda restaria a dúvida: qual juízo seria mais conveniente? Muitas vezes elege-se o foro mais próximo dos escritórios de advogados contratados, porém essa medida pode não ajudar o bom andamento do processo, provocando demoras; o mais correto, principalmente quando os contratos podem gerar demandas em vários países, é eleger o foro que seja capaz de julgar e coagir as partes no caso concreto, porque pode ser muito difícil e demorado fazer-se cumprir uma sentença em local diferente do que a proferiu. Ou seja, é melhor eleger o Foro com capacidade de execução da sentença.

8. Nesse sentido, ver o posicionamento doutrinário de José Rogério Cruz e Tucci em Eficácia probatória dos contratos celebrados pela Internet, in *Direito & Internet*, Edipro, 2001, e Arnoldo Wald, Um novo direito para a nova economia: os contratos eletrônicos e o Código Civil, in

Sendo assim, os requisitos básicos para os contratos eletrônicos terem força probante são: autenticidade⁹ e integridade¹⁰.

Muitos dos contratos em Direito Digital devem ser elaborados caso a caso, de acordo com as necessidades específicas e os direitos e obrigações que devem estar garantidos¹¹.

Contratos de TI

A cada dia que passa estamos mais atrelados à tecnologia. Nos negócios, então, é simplesmente vital; mais vital ainda é a sinergia entre o departamento de TI e o jurídico. Será que o diretor jurídico sabe quem é o diretor de TI e vice-versa? Caso a resposta seja negativa, deveriam saber. Algumas questões interessam e muito para ambos, como: por quanto tempo ficam guardados e-mails? E os logs de acesso?

A parceria dessas áreas na formulação de contratos relacionados ao desenvolvimento de *softwares* e demais usos de TI é o que pode definir uma pendência jurídica no futuro, pois o melhor contencioso é o preventivo.

Pelo conceito clássico, contrato é o acordo de vontades entre duas ou mais pessoas com a finalidade de adquirir, resguardar, modificar ou extinguir direito.

Os contratos “realmente atuais” devem trazer em seu bojo cláusulas de confidencialidade, direitos autorais e propriedade intelectual (em especial, para tratar dos fontes), segurança da informação, prova eletrônica, entre outras. Essa “desatualização” pode implicar o risco de fazer com que o contrato se torne inútil, caso haja um conflito entre as partes.

Direito e Internet, São Paulo: Revista dos Tribunais, 2001. No direito comparado, merece destaque a Lei-Modelo da Uncitral, art. 9º; Decreto-Lei n. 290-D/99, art. 3º, da legislação portuguesa; Utah Digital Act, California Government Code, Section 16.5, Florida Electronic Signature Act of 1996, Georgia Electronic Records and Signatures Act, da legislação americana; Lei n. 59/97, Decreto n. 513/97 e Decreto do Presidente do Conselho de Ministros, de 8 de fevereiro de 1999, da legislação italiana; Real Decreto-Lei n. 14/1999, da legislação espanhola.

9. Autenticidade significa pressuposto da autoria, ou seja, que tenha autoria identificável. Nesse sentido, aplicam-se os arts. 371, I, 368 e 373 do Código de Processo Civil.

10. Integridade significa veracidade, ou seja, que não possa ser alterado depois de pactuado e assinado.

11. Ver Projeto de Lei n. 2.589/2000 (que segundo última consulta ao site da Câmara de Deputados, a posição deste projeto é “em 7/8/2006 — [...] Transformado na Lei Ordinária 11.341/2006. DOU 08.08.06. Pág 04. Col. 01.” Logo, a matéria passou a ser tratada no parágrafo único do art. 541 do CPC. E também o Projeto de Lei n. 3.016/2000 que está apensado ao PL n. 5.403/2001. Vide site <http://www2.camara.gov.br/proposicoes>.

Como já observamos, é aconselhável o uso de um glossário inicial que determine o significado dos termos técnicos empregados no contrato. Isso possibilita uma interpretação mais restrita, em decorrência diminui-se o risco de duplo sentido ou de má compreensão do objeto do contrato. Os contratos, para o Direito digital, têm características peculiares que determinam a necessidade de aprofundar questões normalmente não aplicadas em contratos tradicionais¹².

As espécies mais comuns de contratação são: **1ª) contrato de desenvolvimento de software** — *software* é produto ou serviço? Como vai ser comercializado? Há manutenção e atualizações? Quem será o proprietário do código-fonte? **2ª) contrato hosting** — por quanto tempo as informações serão armazenadas? As informações estarão disponíveis sempre? Existe cláusula de *Backup* dessas informações? Existe uma cláusula de segurança da informação? Caso haja migração como vai ser feita? **3ª) contrato manutenção** — é serviço de manutenção ou de atualização? A manutenção é feita por quem vendeu o *hardware* ou o *software*? **4ª) Contrato de segurança da informação** — caso ocorra um vazamento de informação, quem é responsável? Há cláusula de seguro? A responsabilidade da empresa que faz a segurança é objetiva, ou seja, independe de culpa?

As questões acima são motivo de muita reflexão para aqueles que desejam contratar e preocupação para os que contrataram e colocaram de lado tais questões.

Para finalizar, é bastante oportuno relembrar as peculiaridades deste tipo de contratação: cláusula de irresponsabilidade, glossário, cuidado no uso de imagens ou fotos e cláusula de arbitragem, visto que esses elementos são o sustentáculo de um Contrato de TI bem estruturado e moderno.

- Glossário Preliminar — informação clara, objetiva e definida da terminologia no próprio escopo do documento para evitar subjetividade.

- Cláusula de Prova Digital — acordo entre as partes de que aquela obrigação será provada mediante documentação eletrônica trocada entre elas (*e-mail* etc.).

- Cláusula de obsolescência e atualização da tecnologia.
- Cláusula de segurança de informação (com definição dos padrões).
- Cláusula de privacidade das informações com determinação clara de propósito da coleta, finalidade de uso e prazo de expiração.

12. Ver comentários do item 8.25.

- Cláusula de Direitos Autorais, principalmente no caso da propriedade dos códigos-fonte em desenvolvimentos de *softwares* ou sistemas.

- Cláusula de repasse de informação técnica e documentação — importante caso haja troca de fornecedor no meio ou ao final do projeto.

- Cláusula de mudança, atualização, melhoria ou ajuste — deve prever procedimentos de atualização e controle de versão (no caso de *software*).

- Cláusula sobre acordo de Nível de Serviço — SLA (p. ex.: quando é caso de atendimento de usuário em situação de terceirização de *hosting*, provedor de acesso etc.).

- Cláusula de Identidade Digital — sobre aceitação de uso de processos de reconhecimento de identidade e autenticação (como certificação digital).

- Cláusula de Mediação e Arbitragem, quando for o caso.

- Uso do carimbo do tempo — O carimbo do tempo ASA (Autêntico, Seguro e Auditável) garante que determinado documento existe na data constante do carimbo. Se um *e-mail*, ao ser enviado, foi carimbado, podemos garantir que foi enviado na data do carimbo, nem antes nem depois. O texto que constitui o *e-mail* até poderia existir antes do envio deste, mas quando esse texto passou a fazer parte do *e-mail* que foi enviado, passou a ser passível de comprovação temporal¹³.

13. Para ver carimbo do tempo acessar *website* do Observatório Nacional: <www.on.br> e <www.comprova.com.br>.

Apesar dos estudos específicos sobre contratos, é crescente a necessidade de uma visão mais técnica sobre a capacidade de garantia de níveis de qualidade quando se trata da contratação de serviços de Tecnologia da Informação (TI), Telecomunicações e Energia, já que estes são os três insumos essenciais para a realização da maior parte das atividades e dos negócios na Sociedade Digital.

Logo, este tema exige um estudo mais aprofundado pelo profissional do Direito, bem como pelo gestor da área contratante dos serviços que exigem este tipo de planejamento e preparo prévio, sob pena de, apesar de se ter o contrato, este não responder aos problemas mais comuns envolvidos nestas relações.

A elaboração deste tipo de documento está diretamente relacionada à gestão de riscos contratuais, que exige, por sua vez, estudo de cenários¹. Para tanto, deve-se medir o impacto da contratação no negócio, considerando que determinados tipos de serviços geram impactos distintos para diferentes tipos de empresa. Mesmo contratos de baixo valor podem ter grande impacto nos

1. Recomendação de leituras:

— *Planejamento de cenários*, Kees Van Der Heijden — Editora Bookman;

— *Gerenciamento de riscos* — Paulo Baraldi — Editora Campus;

— *Multisourcing*, Linda Cohen e Allide Young, Gartner, INC, Harvard Business School Press.

negócios. O serviço de hospedagem é essencial para uma loja virtual, assim como o de telecomunicações para uma operadora de cartão de crédito, ou segurança da informação para uma empresa financeira.

Logo, TI designa o conjunto de recursos tecnológicos e computacionais para gestão da informação. A TI é fundamentada nos seguintes componentes: *hardware*, *software*, telecomunicações e gestão de dados e informações.

Por sua vez, como o contrato é um instrumento de circulação de riquezas, e os contratos de TI têm por objeto da contratação um bem/serviço, e já que o TI é um suporte essencial do negócio de pelo menos uma das partes envolvidas, a falha de um contrato pode comprometer o negócio em si² (e em cascata — se fechar um fornecedor quantas outras empresas podem ser impactadas?).

O SLA é, portanto, um documento que declara às partes envolvidas, necessariamente: a) as condições do acordo; b) que serviços de suporte e aplicações estão incluídos; c) quais as penalidades para não cumprimento do acordo; d) como fica o pagamento de honorários; e) qual a política a ser adotada; f) quais os termos de modificações; g) como serão gerados os relatórios, qual frequência, nível de detalhe, e quem deve ler os mesmos; h) quais as responsabilidades de ambas as partes; i) se há previsão de contingência, quando é acionada e que empresa irá atender; j) o que se define por nível de qualidade mínimo daquele serviço entre as partes (podendo ter referência em padrões dispostos em leis, autorregulamentação por Agência Reguladora, ISOs e melhores práticas internacionais; k) cronograma; l) outras questões dependendo do objeto contratual.

O objetivo do SLA é ser uma ferramenta de monitoração e controle do cumprimento do padrão estabelecido no acordo de serviço contratado entre as partes, permitindo deixar de modo claro e inequívoco as expectativas do cliente e as obrigações e limites de responsabilidade do fornecedor. Desse modo, é um instrumento legal e formal para negociação de padrão de fornecimento *versus* condições de fornecimento, e em alguns serviços, especialmente telefonia,

2. *Notícia — Folha de S. Paulo* — “O Estado de São Paulo enfrenta problemas de acesso à internet nesta quinta-feira, com lentidão ou indisponibilidade completa na conexão. A Folha Online apurou que a rede da Telefonica apresenta problemas, gerando reflexos na banda larga, conexões dedicadas (de alta velocidade, utilizadas principalmente por empresas) e outros tipos de acesso. A falha começou a ser sentida na quarta-feira e se intensificou durante a madrugada de hoje. Com isso, a conexão de grande parte dos internautas e das empresas que usam a rede da Telefonica no Estado está instável. Especialistas ouvidos pela reportagem classificaram a pane como ‘grave’ e sem previsão de retorno.” Fonte — <<http://www1.folha.uol.com.br/folha/informatica/ult124u418802.shtml>>, acessado em 3-7-2008.

isso é essencial, já que muitos dos contratos não podem ser alterados, mas há regras de SLA que podem ser customizadas caso a caso³.

Para um bom SLA é fundamental a definição de alguns conceitos, não apenas de termos técnicos, mas também sobre risco e probabilidade⁴.

Os riscos mais comuns na contratação de TI e Telecom são:

- Riscos de desempenho — O bem/serviço não atinge os níveis contratados.
- Riscos de interrupção — Perdas envolvidas na interrupção/restabelecimento do bem/serviço.
- Risco de dependência — Alta especificidade do fornecedor (mercado reduzido).
- Riscos de migração — Decorrentes da troca de fornecedor.
- Risco de má distribuição de estímulos — O contrato tem que sempre estimular a qualidade, não pode ser mais barato entregar bem/serviço de menor qualidade.

3. Fonte: Professor Júlio César C. Ribas — <<http://www.nersd.cefetsc.edu.br/arquivos/seminario01/apresentacoes/sla-slm.ppt>>.

4. A ISO 31000 (*General guidelines for principles and implementation of risk management*) visa à padronização de processos que permitam o gerenciamento dos riscos de modo mais holístico. Consiste em um conjunto de diretrizes para padronizar modelo de processo de tomada de decisão em gerenciamento de riscos (conceitos, terminologias, procedimentos). É uma norma de alto nível — não concorre com as demais normas já existentes. O texto original da ISO 31000 foi baseado na norma AS/NZS 4360:2004. Traz uma visão integrada de ERM — *Enterprise Risk Management*. No Brasil, a ABNT — Associação Brasileira de Normas Técnicas — criou a Comissão de Estudo Especial Temporária para a Gestão de Riscos — coordenação do Alberto Bastos. Traz um rol de conceitos:

- Risco é a possibilidade de ocorrência de um evento ou de suas consequências.
- Probabilidade conceitualmente é o mesmo que chances ou possibilidades.
- Um evento pode ocorrer ou pode ser um conjunto de circunstâncias a ocorrer.
- Consequências são definidas em termos dos objetivos da empresa. Elas podem ser incertas.
- O nível de risco pode ser qualquer combinação entre possibilidade e consequência definida conforme os objetivos da empresa. Ela precisa ser (ou deveria ser) calculada com base em valores estimados.
- O critério de risco especifica como combinar possibilidade e consequência para estimar o nível de risco.
- O tipo de risco é definido pela noção de causa e efeito, e se o risco for negativo, a base de definição é o dano.
- Risco residual é o risco remanescente após a empresa ter tratado o risco.

- Riscos trabalhistas — Decorrentes da equipe alocada (mão de obra do fornecedor).
- Riscos de comprometimento de ativos — que inclui perdas de dados, inclusive quebra de confidencialidade e SI.

Uma questão fundamental quando da feitura de um SLA é: a gestão de risco vai afetar a economia do contrato? Vale a pena? Estamos acrescentando custos ou minimizando os “custos invisíveis”? Além disso, o gerenciamento dos riscos deve se fazer ao longo de todo o projeto (pré, durante e pós), desde a especificação até a leitura das métricas apresentadas nos relatórios. Se o contrato não for de prestação de serviço continuado, tiver prazo para encerrar, é essencial a entrega da documentação técnica completa ao final.

Muitos dos riscos não identificados que geram “custos invisíveis” e aumentam ao longo do tempo do projeto afetando profundamente a empresa são causados por falta de informação (falhas na especificação preliminar do projeto), falta de gestão adequada do contrato/projeto ou falta de decisão ou demora da decisão quando há um incidente devido aos riscos de mudança ou não existência de Plano de Continuidade (famoso plano B).

Na definição das cláusulas de responsabilidade, deve-se ter em mente que o melhor é sempre o mais barato e eficiente. Então a pergunta a ser feita no momento da redação das cláusulas é: quem pode gerenciar os riscos da atividade de forma mais eficiente e com o menor dispêndio de recursos? O estudo de cenários a ser feito, deve considerar: a) de quem é o risco do negócio; b) o que é melhor — assumir os riscos, repassar todos os riscos ao fornecedor, compartilhar os riscos, delimitar um teto de valor; c) qual o impacto financeiro do “fazer ou não fazer”.

Para gerar controle dos riscos, é comum o uso de cláusulas no SLA que tratem de: multas por desempenho insuficiente, monitoramento ostensivo, redundância e contingenciamento, *co-sourcing* (ter mais de um fornecedor) para evitar concentração, acordos de *fase-in* e *fase-out* (para entrada e saída), ganho por desempenho (SLA compensatório), garantias e seguro (quando aplicável).

Mas todo contrato de TI precisa destes controles? Normalmente, exceder os controles significa despendar mais recursos que os necessários. Logo, o gerenciamento adequado dos riscos, que é justamente a espinha dorsal de um SLA, significa, no mínimo, entender quais os riscos envolvidos, dimensionar o impacto dos mesmos no negócio, definir sua origem e de quem é a responsa-

bilidade originária (incluindo aqui a análise de “risco do próprio negócio⁵”), para então poder mitigá-los de modo eficiente.

É muito comum não haver uma avaliação jurídica da parte técnica, e vice-versa, no momento certo, para feitura do SLA. Como escrever a cláusula faz toda a diferença⁶. Por isso, os erros mais comuns são: a) determinar um SLA

5. Situação de eventual responsabilidade objetiva, conforme reza o art. 14 do Código de Defesa do Consumidor: “O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos”.

6. Exemplo de cláusulas que devem constar em SLA:

Assistência na Transferência:

Cláusula XX — A CONTRATANTE irá obter assistência da CONTRATADA na transferência dos Serviços para a própria CONTRATANTE, suas Afiliadas ou um Terceiro quando da rescisão ou expiração deste Contrato (Assistência na Transferência), mediante solicitação por escrito da CONTRATANTE à CONTRATADA, que prestará essa Assistência na Transferência à CONTRATANTE, na medida em que a CONTRATADA:

a) possa prestar essa Assistência na Transferência solicitada empregando seus recursos então existentes, destinados exclusivamente à prestação dos Serviços sob este Contrato, até a expiração ou rescisão deste Contrato; e

b) concorde em prestar a Assistência na Transferência, pelo período de tempo solicitado pela CONTRATANTE, período esse não será superior a seis meses após a Data de Expiração ou rescisão deste Contrato (o Período de Assistência na Transferência).

Cláusula XX — Durante o Período de Assistência na Transferência, a CONTRATADA concederá à CONTRATANTE, a suas Afiliadas e a seus Terceiros, conforme necessário, razoável acesso às Máquinas e ao Software, desde que:

a) esse acesso não interfira na capacidade da CONTRATADA de prestar os Serviços ou a Assistência na Transferência; e

b) esses Terceiros e as Afiliadas da CONTRATANTE cumpram as exigências de segurança e confidencialidade da CONTRATADA.

Rescisão Contratual:

Cláusula XX — O presente Contrato poderá ser rescindido a qualquer tempo, pela CONTRATANTE, mediante comunicação formal à outra parte, com antecedência mínima de 60 (sessenta) dias.

A CONTRATADA não poderá rescindir unilateralmente o presente Contrato, salvo mediante comunicação formal à outra parte, com antecedência mínima de 6 (seis) meses, obrigando-se ainda a prestar os serviços necessários para transição de prestador(es) dos serviços deste Contrato.

Plano de Contingência:

Cláusula XX — A CONTRATADA, para cumprimento deste contrato, obriga-se a criar mecanismos de contingência, observando os mesmos parâmetros utilizados pela CONTRATANTE, cabendo-lhe apresentar por escrito esse Plano de Contingência, devendo testá-lo e mantê-lo atualizado semestralmente. O Plano de Contingência deverá conter a título meramente exemplificativo:

- Plano de ação para impossibilidade de acesso ao local onde os serviços objeto deste contrato estiverem sendo prestados.
- Plano de ação para impossibilidade de locomoção (exemplo: greves de transportes, inundações).
- Plano de ação para greve geral de trabalhadores ou da categoria funcional dos profissionais alocados na prestação dos serviços, inclusive da CONTRATADA, quando isto possa afetar o

restritivo e não implementar relatórios de monitoramento/desempenho, pois sem o acompanhamento preciso o SLA perde toda utilidade; b) pensar o preço de modo equivocado, logo o preço do serviço prestado é igual ao do serviço não prestado; c) não pensar o impacto da data em si da ocorrência no negócio (será que ter o serviço interrompido de madrugada gera o mesmo impacto que às vésperas do natal, no fim de semana, para uma loja?); d) a contratante de grande porte querer transferir todos os riscos para a contratada de pequeno porte; e) não documentar as infrações ao longo do contrato; f) negligenciar a resolução amigável que é mais fácil de ocorrer quanto melhor tiver sido a gestão do contrato e a documentação da prestação do serviço; g) para serviços críticos ter apenas uma cláusula de rescisão pelo fornecedor sem levar em consideração o tempo real de substituição do mesmo e o período de migração necessário, fazendo o contratante, indiretamente, ficar refém do contratado.

No tocante à jurisprudência de nossos tribunais pátrios que apontam a interrupção dos serviços como causa para a reparação de danos incluindo os de ordem moral⁷, não há como celebrar contratos com cláusulas que excluam

bom andamento dos trabalhos.

- *Os procedimentos e as prioridades para ativação do plano e a especificação das atividades a serem realizadas.*
- *Os nomes, endereços e telefones das pessoas responsáveis pela CONTRATADA autorizadas a efetuar a ativação do Plano de Contingência.*
- *Os procedimentos sobre backups diário, semanal e mensal dos sistemas, indicando inclusive o sistema utilizado, quando aplicável.*
- *Os critérios e sistemas utilizados para segurança das informações dos sistemas e dados que estiverem a seu cargo.*
- *Forma e periodicidade dos testes de contingência e comprovantes de sua realização, inclusive de recuperação de dados e segurança de informações.*

7. Jurisprudências:

“PRESTAÇÃO DE SERVIÇOS — INDENIZAÇÃO — TELEFONE — INTERRUPÇÃO SEM JUSTA CAUSA — DANO MORAL — CARACTERIZAÇÃO — RECURSO NÃO PROVIDO. A privação do direito de uso de terminal telefônico, sem justa causa, traz não só dissabores ao consumidor, mas sim sensação de angústia, menos valia, sofrimento moral, em suma, dor na alma, caracterizadora de dano moral, a merecer compensação, de sorte, não só a aplacar o sofrimento da vítima, como servir de punição ao agente causador e fator de educação, para que não reincida no erro” (TJSP, Ap. 1114984-0, Rel. Des. Paulo Ayrosa, j. 29-1-2008).

“OBRIGAÇÃO DE FAZER — INDENIZAÇÃO — TELEFONIA — PESSOA JURÍDICA — DANO MORAL — Civil. Consumidor. Administrativo. Processual Civil. Demanda de obrigação de fazer, com preceito cominatório, de declaração negativa de débito, e indenizatória na esfera moral. Grande empresa mercantil sediada na Capital de São Paulo, em seu nome e no de filiais naquele Estado, Goiás e Rio Grande do Sul, insurgindo-se contra falha na prestação de serviços de telefonia fixa em grande distância (DDD e DDI), de que decorreram inscrições cadastrais negativas em órgão protetivo do crédito. Tutela antecipada parcial. Senten-

completamente a responsabilidade do prestador, sobre qualquer coisa provocada pelo mau fornecimento do serviço⁸. A questão que se coloca é, o que é

ça de procedência. Apelação. Sendo a Ré, Embratel, prestadora maior dos serviços referidos, acoplado seu sistema ao de empresas operadoras regionais, sendo também delegatária de tais serviços, que são públicos, da União, sua responsabilidade é objetiva, à luz do artigo 37, § 6º, da Carta da República, como do Código de Defesa do Consumidor (Lei n. 8.078/1990). Assim se fulcra no risco administrativo o negocial, esse por sua maior força econômica. Invertido o ônus probatório para o favorecer da pretensão, não da resistência. (...) Dano moral de ser reparado às pessoas jurídicas, não só às físicas, consoante cediço entender pretoriano, máxime do Egrégio STJ. Ocorrência *in re ipsa*, também notada por experiência. Lesão manifesta à imagem social e comercial da Autora. Sentença que deve ser mantida na maior parte, reformada na menor. (...)” (Ap. Cív. 2004.001.09132, TJSP, 3ª Câmara Cív., rel. Des. Paulo Ayrosa, j. 22-6-2004).

“Consumidor — Telefone — Condomínio — PABX Serviço não fornecido — Conta não paga — Faturamento antigo — Dano moral. O prestador do serviço responde pela prestação contratada, mas quando há falha e esta não lhe compete, ocorrendo segundo alega por culpa de terceiro é sua incumbência fazer tal demonstração. Ao se omitir responde como lhe foi imputado pelo consumidor. Hipótese de administrador de rede de PABX telefônico de condomínio que alega que o não funcionamento do serviço se deveu a problemas da rede externa administrada pela cia. telefônica (Telemar). Indenização por dano moral nessa parte procedente, mas não pode na sentença o Juiz isentar o assinante do pagamento das ligações pendentes, sob a alegação de faturamento depois de 90 dias, já que decidiu sem suporte algum quer no contrato, quer na lei” (Ap. Cív. 2005.001.22772, TJRJ, 14ª Câmara Cív., rel. Des. Rudi Loewenkron, j. 18-10-2005).

“TELEMAR — CONTRATO DE TELEFONIA — CORTE INDEVIDO DO SERVIÇO — FALHA NO SERVIÇO CONFESSADA PELA RÉ — DANO MORAL CONFIGURADO — DANO MATERIAL CARECEDOR DE COMPROVAÇÃO. Não se faz necessária a comprovação do desequilíbrio funcional de ente coletivo que se afirma lesado, pois o desajuste de tal índole constitui corolário da própria funcionalidade empresarial. Quanto aos alegados danos materiais, estes sim necessitam de comprovação, não bastando a mera alegação. Parcial provimento ao recurso” (Ap. Cív. 2006.001.09731, TJRJ, 17ª Câmara Cív., rel. Des. Edson Vasconcelos, j. 26-4-2006).

“Indenização por Danos Morais. Empresa operadora de telefonia de longa distância (EMBRATEL), que usa o cadastro de usuários da empresa de telefonia local (BRASIL TELECOM) para emitir suas próprias faturas. Fraude praticada por desconhecido que, por telefone, usando o nome e dados pessoais do autor da ação, contrata com a segunda o serviço de telefonia fixa, deixando de pagar as faturas emitidas pela primeira, vindo esta a inscrever o nome do autor no Serviço de Proteção ao Crédito. Dano moral configurado. Responsabilidade objetiva e solidária das apelantes. Indenização devida. 1. As empresas de telefonia, local e de longa distância, que atuam conjuntamente no mercado, respondem solidária e objetivamente perante o consumidor, por danos causados a este em razão das falhas do serviço. 2. Se a empresa de telefonia local, para diminuir os custos e maximizar os lucros, elimina postos de atendimento pessoal, passando a contratar o fornecimento de serviços por telefone, pelo sistema apelidado *call center*, sem conferir a veracidade dos dados pessoais fornecidos pelo solicitante do serviço, assume todos os riscos daí decorrentes, inclusive o de ser responsabilizada por eventuais danos causados aos consumidores, pela falha do serviço. (...)” (ACJ 2004.071.0198433, DF, 1ª Turma Recursal dos Juizados Especiais Cíveis e Criminais, j. 10-5-2005).

8. Ainda que não se entenda estarmos diante de relação de consumo, incidem no caso, as normas do Código Civil, que regem os contratos e o direito obrigacional:

o “mau fornecimento”, o que pode ser entendido como “caso fortuito ou de força maior”, sob pena de a minuta ser derrubada quando submetida aos Tribunais. Afinal, o papel aceita tudo.

Este assunto é extremamente relevante e deve ser bem compreendido para que se possa de fato fazer uma adequada blindagem legal na contratação de serviços de TI e Telecomunicações em geral. Sem isso, o contrato não tem qualquer serventia.

Art 186. “Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”.

Art. 421. “A liberdade de contratar será exercida em razão e nos limites da função social do contrato”.

Art. 422. “Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé”.

Art. 423. “Quando houver no contrato de adesão cláusulas ambíguas ou contraditórias, deverá-se adotar a interpretação mais favorável ao aderente”.

Art. 427. “A proposta de contrato obriga o proponente, se o contrário não resultar dos termos dela, da natureza do negócio, ou das circunstâncias do caso”.

Art. 439. “Aquele que tiver prometido fato de terceiro responderá por perdas e danos, quando este o não executar”.

Artigo 927. “Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo”.

Primeiramente, vamos analisar o conceito tradicional do instituto da arbitragem, que sabemos ser muito antigo dentro do mundo jurídico. Assim, resumidamente, a arbitragem consiste num acordo de vontades para a criação de um juízo privado não pertencente à jurisdição estatal, escolhido pelas partes para dirimirem questões presentes ou futuras sobre direitos disponíveis, entre elas, sobretudo relativos a contratos.

Como afirmamos, o instituto jurídico da arbitragem não é recente. Sua origem remonta aos primórdios da jurisdição, na Grécia antiga, existindo referências a ela em escritos de Platão, Aristóteles e Demóstenes. Também entre os romanos a arbitragem foi mantida como jurisdição privada, funcionando paralelamente à jurisdição estatal. Isso porque o *jus civilis* era aplicado somente aos cidadãos romanos; as outras pessoas tinham de remunerar o árbitro, visto que o império não dava este direito de cidadania aos plebeus: um juiz remunerado.

Esta característica da arbitragem e a escolha do árbitro pelas partes, e assim como a escolha do direito a ser aplicado no caso concreto, são os fundamentos do instituto e permaneceram praticamente inalterados até a atualidade.

Em nosso ordenamento jurídico, a arbitragem está disciplinada desde a Constituição do Império de 1824, passando pelo Código Civil de 1916, de 2002 e pelos Códigos de Processo Civil de 1939 e 1973. No entanto, a prática da arbitragem no Brasil nunca teve a mesma importância que assume em outros países, sobretudo nos mais desenvolvidos, por uma série de fatores, podendo-se

destacar como o mais importante a própria dificuldade gerada pela incapacidade de execução da cláusula e/ou compromisso arbitral, bem como pela obrigatoriedade de homologação judicial do laudo nacional e da dupla homologação do laudo estrangeiro, que eram vigentes em período anterior.

Com o advento da Lei n. 9.307, de 1996, a nova Lei de Arbitragem no Brasil, que revogou os artigos do antigo Código Civil e do Código de Processo Civil que anteriormente regulavam o instituto, a arbitragem passou a ser mais aplicada no direito brasileiro. A nova lei trouxe alterações benéficas e um novo ânimo à questão da arbitragem, possibilitando em nosso país o mesmo desenvolvimento da justiça privada e as vantagens a ela inerentes.

Uma das características mais importantes do juízo arbitral é a possibilidade de escolha das regras, da base legal para o julgamento da lide, em que as partes podem dispor sobre qual a legislação aplicável na resolução de determinada controvérsia, de acordo com os usos e práticas comerciais, ou até mesmo pela equidade, pelo livre convencimento do árbitro sobre o que é justo. De fato, as partes podem escolher livremente o critério para o arbitramento, limitadas apenas pelo respeito à ordem pública e aos bons costumes. Convém lembrar que, uma vez escolhidas as regras, a decisão arbitral e o árbitro estão vinculados à observação delas.

Existem dois mecanismos pelos quais as partes acordam em resolver suas questões mediante um árbitro: (i) a cláusula arbitral; e (ii) o compromisso arbitral (judicial ou extrajudicial). A cláusula arbitral é um pacto firmado em um contrato no qual as partes decidem que as possíveis futuras questões oriundas de determinada relação contratual serão dirimidas mediante arbitragem. A cláusula pode ainda estar em documento separado do contrato original, desde que a ele se refira, e por considerar-se esta autônoma em relação ao restante do contrato principal, consequentemente, a nulidade de um não implica, necessariamente, a do outro. Por sua vez, o compromisso arbitral é o acordo firmado para a resolução de controvérsia já existente sobre determinado contrato. Se a questão ainda não foi levada ao Poder Judiciário, o compromisso é extrajudicial; se firmado no decorrer do processo em andamento, o compromisso arbitral é judicial e encerra o processo sem resolução de mérito (inciso VII do art. 267 do CPC).

Para nós, uma das alterações mais importantes trazidas pela Lei n. 9.307/96 refere-se à executividade¹ da cláusula arbitral, de tal sorte que, uma vez acor-

1. Muito se questionou a respeito deste mecanismo da nova lei (arts. 6º e 7º) e da sua incompatibilidade com o princípio constitucional contido no art. 5º, XXXV, que diz: "A lei não

dados, os litígios deverão ser resolvidos por juízo arbitral, podendo uma das partes compelir a outra a submeter-se à arbitragem, por meio do Poder Judiciário. Neste sentido, o art. 7º da Lei n. 9.307/96 estabelece o procedimento próprio para que a parte interessada requeira o comparecimento da outra parte para lavrar-se o compromisso arbitral.

Outra principal inovação é o arrolamento da sentença arbitral como título executivo judicial (inciso IV do art. 475-N do CPC), podendo ser promovida a execução forçada de plano, dispensando-se o burocrático procedimento de homologação.

De acordo com a Lei n. 9.307/96, a sentença arbitral não é passível de recurso nem de homologação pelo Poder Judiciário; entretanto, poderá ocorrer nulidade da decisão arbitral, se constatada qualquer das hipóteses do art. 32² da referida lei.

Para o Direito Digital não existe melhor forma de resolução de conflitos que o uso dos mecanismos legais de arbitragem e mediação. As vantagens do juízo arbitral vêm ao encontro das necessidades geradas pelas novas formas de relacionamento na sociedade digital, principalmente no tocante à celeridade dos processos e ao conhecimento específico envolvido em cada caso.

Em primeiro lugar, a própria lógica do juízo arbitral é de dar a menor sanção possível e a máxima recomposição dos prejuízos, de modo que a sentença arbitral não costuma trazer surpresa às partes com indenizações desproporcionais. Acrescente-se o fator tempo, já que as decisões arbitrais podem sair em poucos dias ou no máximo em seis meses, salvo se outro prazo for conveniado pelas partes (art. 23 da Lei n. 9.307/96); na sociedade digital o custo de um longo tempo em litígio pode superar, muitas vezes, o valor da própria causa, tornando cada vez mais verdadeiro o brocardo "*justiça tarda é justiça falsa*".

Lembramos ainda que a escolha do árbitro pode ser fundamental para o resultado justo da arbitragem, pois viabiliza a seleção de pessoas com notório

excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito". Contudo, o STF decidiu pela constitucionalidade do referido diploma legal.

2. Lei n. 9.307/96 (Lei de Arbitragem), art. 32. "É nula a sentença arbitral se: I — for nulo o compromisso; II — emanou de quem não podia ser árbitro; III — não contiver os requisitos do art. 26 desta Lei; IV — for proferida fora dos limites da convenção de arbitragem; V — não decidir todo o litígio submetido à arbitragem; VI — comprovado que foi proferida por prevaricação, concussão ou corrupção passiva; VII — proferida fora do prazo, respeitado o disposto no art. 12, III, desta Lei; e VIII — forem desrespeitados os princípios de que trata o art. 21, § 2º, desta Lei".

conhecimento na área, que muitas vezes requer saber técnico alheio aos que se podem, razoavelmente, esperar de um juiz togado.

Observamos que, quanto à aplicabilidade, a área que mais necessita de arbitragem nas questões de Direito Digital é, talvez, a das transações comerciais, ou seja, os contratos de *e-commerce* (ressaltamos também importância da arbitragem para as questões de disputa de domínio). Ora, como a arbitragem permite que as partes não só definam a jurisdição, uma vez que a arbitragem pode ser também internacional, mas também a legislação aplicável ao caso, a inclusão de uma cláusula arbitral nos contratos eletrônicos seria a melhor maneira de resolver eventuais litígios.

Acreditamos que o instituto ainda irá evoluir muito e ser cada vez mais utilizado. É o processo contínuo de aprendizado que constrói uma sociedade sólida e um Direito eficaz. É nisso que estamos trabalhando.

Na sociedade digital, o advogado tem de ser um estrategista. A complexidade da sociedade traz maior complexidade jurídica. Já não é suficiente conhecer apenas o Direito e as leis; devem-se conhecer os modelos que conduzem o mundo das relações entre pessoas, empresas, mercados, Estados. A postura profissional de estrategista significa assumir um papel determinante para a adequada condução dos negócios no mundo digital. Cabe ao profissional do Direito dar os caminhos e as soluções viáveis, pensadas no contexto competitivo e globalizado de um possível cliente virtual-real, convergente e multicultural.

Saber estabelecer estratégias jurídicas eficientes no mundo cada vez mais digital e virtual é condição de sobrevivência do profissional do Direito, dado que cada vez mais o tempo e a tecnologia atuam de modo a exigir celeridade e flexibilidade nas soluções jurídicas. A questão que se coloca é de eficácia. Para isso, devemos antever os acontecimentos, preparar os contratos de modo flexível para que sobrevivam às mudanças rápidas que a sociedade atravessa, para não se tornarem obsoletos logo após sua assinatura.

Nesse contexto, cada vez mais, o advogado deve ter visão e conduta de negociador. Já não cabe uma visão contenciosa ou legalista. Em sua formação, passa a ser importante saber dominar as novas ferramentas e novas tecnologias à disposição, estudar as inter-relações comerciais e pessoais que ocorrem na Internet e nas novas mídias interativas como celular, tv digital e outras, além de ser essencial que tenha o conhecimento global de todas as disciplinas do

Direito Digital, com suas novas linguagens, terminologias e códigos. Além disso, precisa ter ainda uma visão ampla do universo jurídico e entender o movimento de autorregulamentação e sua legitimidade, a substituição de leis por *softwares* que regulam condutas e comportamentos na rede, as mudanças do conceito de soberania em um mundo globalizado e virtual, a necessidade de incentivos à livre-iniciativa virtual (*e-commerce*), as questões de importação de bens não materiais via Internet e seu impacto macroeconômico, as situações de consumidores virtuais, entre outros.

Portanto, verificamos que a informatização tem trazido aos profissionais do Direito mudanças não só na maneira de pensar o direito, mas também de trabalhar com ele. Com a informatização dos escritórios e do próprio Poder Judiciário, assim como as profundas alterações em sede processual, não podemos admitir que os juristas não estejam preparados para compreender e discutir essas novas questões. Talvez este seja o momento de pensar em como as Faculdades de Direito devem formar operadores jurídicos, exigindo que eles tenham um mínimo de conhecimento técnico a respeito das mudanças dos paradigmas e forte base teórica sobre os princípios que regem a nova era digital e suas implicações.

Ser um jurista nesta nova era pode significar ter de mediar uma situação tal como a seguinte: os Estados Unidos rejeitaram, recentemente, um compromisso internacional sobre repartição de custos entre provedores do tráfego global de Internet. Que implicação isto tem, para nós e para o Direito Digital? Pelo sistema em vigor, os provedores estrangeiros pagam o custo total da conexão para os Estados Unidos, embora o tráfego seja bidirecional. Estamos falando de um custo anual de bilhões de dólares para pagar o tráfego da Internet gerado por usuários nos Estados Unidos, conta esta que deve ser paga pelos outros países. Não seria uma nova forma de imperialismo? Qual o preço que os países em desenvolvimento devem pagar por esta modernidade? A que custo social? Como equilibrar a balança de pagamento com a crescente saída e entrada de produtos e serviços virtuais? Como equilibrar os juros quando importamos tecnologia e mão de obra qualificada e ainda temos de pagar pelo fluxo de informação que sai do País em direção aos Estados Unidos via Internet? Quando temos de pagar a conta da implantação de *backbones* submarinos? Se não é o Estado que paga, é a sociedade, são as empresas, o que, de qualquer modo, acaba por refletir nos preços, nos custos operacionais, na capacidade competitiva, na diminuição da margem de lucro, no desemprego, na recessão.

Como lembra Peter Drucker, se o conhecimento já não tem fronteiras, como garantir o direito de propriedade, que é o que autoriza ao Estado o Poder

de Polícia, que é o que justifica a força pela defesa da Soberania, que é o que nos faz civilizados? Seria obrigação dos governos resolverem essas questões no âmbito internacional? Seria uma obrigação de o Itamaraty defender os interesses dos brasileiros ao livre acesso a baixo custo do tráfego mundial de informação? Teriam todos os cidadãos do mundo o direito a participar desta cadeia de globalização? Como equilibrar o analfabetismo digital?

Situações como esta, em caráter supranacional, e muitas outras, principalmente no tocante a relações comerciais e relações com o consumidor, serão cada vez mais comuns e mais complexas. Nós, operadores do Direito, temos a obrigação de participar ativamente do processo de adaptação jurídico-social a estas e muitas outras questões. Não podemos estar à margem dessa transformação, sob pena de estarmos endossando o fim do Estado de Direito.

No contexto do novo profissional do Direito, estrategista, informatizado, com visão de negociador, devemos abordar mais um aspecto que tem gerado controvérsias, o referente aos serviços jurídicos prestados *online*. Atualmente, existem mais domínios de profissionais liberais registrados para advogados do que qualquer outro ramo, ultrapassando até mesmo os profissionais de tecnologia de informação.

A Ordem dos Advogados do Brasil reconheceu a importância das páginas pessoais¹, para divulgação do escritório, dos serviços e até para que se disponibilizem informações aos clientes, mediante senha, sobre os processos, mas o Tribunal de Ética da OAB não permite a consulta a advogados por meio eletrônico, pois acredita que a relação com o cliente deve ser sempre pessoal. Agora, é importante saber o que significa exatamente uma "relação pessoal". Ou corremos o risco de não podermos tratar com advogados por telefone, por exemplo.

Outro entendimento teve a American Bar Association, órgão equivalente à OAB nos Estados Unidos, que já autorizou a operação do *site* Lexuniversal (www.lexuniversal.com), que é uma rede que reúne 50.000 profissionais de renomados escritórios localizados em diferentes países. Criado pelo advogado brasileiro Ordélio Azevedo Sette, o *site* disponibiliza praticamente todos os serviços que podem ser prestados num escritório convencional, como uma consulta com advogados, e ainda desfruta das vantagens operacionais típicas dos negócios na rede, como a redução de custos e a celeridade.

1. Provimento OAB n. 94/2000, que dispõe sobre a publicidade, a propaganda e a informação da advocacia.

Devemos ter uma visão crítica sobre a formação do operador do direito atual. Na verdade, quem se forma em uma Faculdade de Direito, da forma como é ainda ensinado, já ingressa no mercado de trabalho desatualizado. O conteúdo programático das disciplinas de graduação precisa ser revisto para poder estar mais aderente com as novas exigências da Sociedade Digital.

Como aprender Direito Constitucional sem ter horas-aula para explicar como fica a privacidade e o monitoramento? Ou mesmo a questão da liberdade de expressão e a vedação ao anonimato em uma época em que é comum haver tantas ofensas digitais e crimes contra honra em *blogs* e comunidades? Ou até mesmo o princípio da identidade digital ou a necessidade de proteção das fronteiras informacionais?

Como compreender a demanda atual do Direito do Trabalho sem ser orientado sobre qual a possibilidade jurídica de uso de um *e-mail* como prova, ou como fazer os quesitos para uma perícia em ponto eletrônico? Ou o estudo aprofundado das novas relações jurídicas oriundas do teletrabalho e do trabalho remoto²? O assunto relacionado ao teletrabalho virou lei no final do ano de 2011, levando a alteração do art. 6º da Consolidação das Leis do Trabalho. A nova redação equipara o empregado que está presencialmente na empresa àquele que trabalha de forma remota, no modelo *home office*. Essa mudança na norma apenas formalizou o entendimento jurisprudencial, de ser indiferente onde fisicamente está o funcionário para que ele tenha os mesmos direitos previstos na legislação trabalhista.

A redação dada no artigo³ levou a uma interpretação de que o recebimento da mensagem já configuraria colocar o funcionário em trabalho, impac-

2. A Súmula 428 do TST tratou recentemente a respeito do sobreaviso de empregados que utilizam aparelhos eletrônicos (BIP, *pager* ou aparelho celular) para comunicar-se e isto não caracteriza o instituto de sobreaviso, pois não permanecem em sua residência. Súmula 428: Sobreaviso (conversão da Orientação Jurisprudencial n. 49, da SBDI-1). “O uso de aparelho de comunicação, a exemplo de BIP, *pager* ou aparelho celular, pelo empregado, por si só, não caracteriza o regime de sobreaviso, uma vez que o empregado não permanece em sua residência, aguardando, a qualquer momento, convocação para o serviço”.

3. A redação do art. 6º da CLT foi dada pela Lei n. 12.551/2011, que diz:

Art. 6º Não se distingue entre o trabalho realizado no estabelecimento do empregador, o executado no domicílio do empregado e o realizado a distância, desde que estejam caracterizados os pressupostos da relação de emprego.

Parágrafo único. Os meios telemáticos e informatizados de comando, controle e supervisão se equiparam, para fins de subordinação jurídica, aos meios pessoais e diretos de comando, controle e supervisão do trabalho alheio.

tando o entendimento sobre hora extra e sobreaviso quando o funcionário recebesse a informação após o horário normal do seu turno ou expediente. A interpretação é retirada do texto de lei, mas pode impactar muito o modelo de trabalho da sociedade digital, uma vez que a interpretação tende a ser mais favorável aos interesses do empregado.

A informação circula independente de horário, especialmente com o aumento da força de trabalho da chamada geração Y, em que o próprio empregado possui recursos de mobilidade, mesmo que a empresa não tenha oferecido como ferramenta de trabalho. As empresas têm sido obrigadas a bloquear o acesso do colaborador quando ele sai de férias, pois as pessoas estão cada vez mais conectadas e ligadas, o tempo todo, e não querem esperar o dia seguinte ou o início do expediente para saber o que está acontecendo ou para tomar providências proativas de trabalho. Mesmo que seja por liberalidade do próprio profissional que, em um mercado mais competitivo, sem fronteiras e de alcance global, queria mostrar serviço, mesmo que a empresa não tenha solicitado.

Pela interpretação da norma, três situações podem ocorrer quando um colaborador recebe uma mensagem relacionada a trabalho após o expediente, pelo fato de conseguir acessar seu *e-mail* corporativo, por seu *smartphone* ou dispositivo similar: (i) entender que essa hora de serviço à disposição da empresa deve ser paga como sobreaviso (o trabalhador receberia pelo período, à equivalência de um terço do salário); (ii) considerar como hora normal de trabalho; (iii) não pagar nada pelo serviço à disposição e analisar essa questão sob a ótica do tipo de recurso (celular, *pager*, *e-mail*, telefone fixo, redes sociais etc.).

A suspensão dos recursos tecnológicos significam um retrocesso, podendo gerar perda de talentos, frustração na dinâmica de relacionamento entre as equipes e as chefias, empobrecimento do modelo de trabalho e diminuição da competitividade do Brasil e da oferta de empregos, além de poder impactar na indústria de TI e Telecom, com a possível queda dos recursos intrínsecos à mobilidade.

Essa alteração na CLT quis consolidar o trabalho remoto, mas acabou impactando o *mobile office*, ou seja, o comportamento do trabalho na era da mobilidade, em que o profissional quer receber seus *e-mails* corporativos no *smartphone* e estar a par do que ocorre no âmbito profissional, mesmo que não tenha sido solicitado para tanto. Se o mero recebimento de um *e-mail* for igual a uma ordem direta, independentemente do conteúdo, do que foi solicitado, muitas empresas poderão suspender ou bloquear o acesso fora do horário de expediente. Esse reflexo torna o Brasil menos competitivo, isto é, querer antecipar a conversa, a informação, o que é recorrente no dia a dia torna-se um risco de se caracterizar hora extra e sobreaviso.

A regra não se aplica a cargos de confiança, claro, mas pense que um novo profissional, que é da geração Y e possui seu próprio celular, troca mensagens de texto com outros integrantes da equipe e até mesmo com seu chefe, e que essa troca de informação só possa ocorrer no horário definido da jornada de trabalho ou que tenha de ser pago adicional por hora extra ou sobreaviso. As pessoas já trabalham a qualquer hora e de qualquer lugar, muitas vezes por conveniência própria.

Esse comando vai na contramão do que é preciso ajustar na legislação trabalhista, que precisa evoluir e permitir jornada flexível, regras definidas entre as partes, e que empregador e empregado possam combinar como será o trabalho sem receio de que isso seja alterado no judiciário posteriormente.

Logo, é necessário que o empregador e o empregado regulem essa atividade. A falta de regra interna própria definida com o advento da nova Lei acarretará um clima de insegurança sobre o regime de trabalho e o receio de condenação para o pagamento de verbas adicionais, pois é praticamente impossível controlar a circulação da informação.

É estranho aprender Direito Comercial sem que seja feita qualquer menção ao comércio eletrônico, às tendências de serviços pelo celular, tais como *mobile banking*, entre outros, ou o próprio Direito do Consumidor sem análise de leis e jurisprudências que envolvem o consumidor *online*. Ou deixar de ver no Direito Concorrencial a espionagem eletrônica e o furto de tráfego com desvio de clientela em buscadores utilizando indevidamente a marca de concorrente direto de mercado.

Há lacunas de ensino que determinam um prejuízo ainda maior à formação do aluno, tais como a área de Direito Penal e de Direito Civil, neste último, especialmente a parte de Direito Autoral. Desse modo, formam-se profissionais que não sabem definir autoria em ambientes eletrônicos em que as testemunhas são máquinas, ou mesmo solicitar evidências relacionadas a IPs e *logs* para as empresas provedoras de serviços de acesso a Internet.

Em uma contratação entre uma empresa e um programador, de quem é o direito sobre os códigos fontes de um *software*? Qual a relevância na definição jurídica clara dos conceitos de atualização, melhoria, customização em um contrato relacionado a TI. O que é um SLA em um contrato de Telecomunicações? O que significa o princípio do *fair use* na cópia de uma mídia original para uma de manuseio?

Na análise dos temas de Direito Tributário, como não debater sobre a tributação ou não de *download*, já que o mesmo conteúdo, quando entra fisicamente pela fronteira, deve recolher o imposto de importação? Ou ainda,

saber quais os incentivos para a indústria de tecnologia, já que o país precisa crescer na produção e exportação de *software* se quiser competir no mundo globalizado.

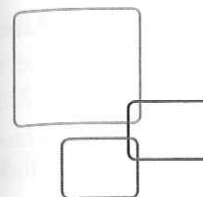
Em uma avaliação ainda mais profunda, verificamos que as Faculdades de Direito não ensinam empreendedorismo, não capacitam os alunos a montarem seus próprios escritórios jurídicos, já que este país precisa de empregos gerados pela iniciativa privada e não só candidatos a cargos públicos.

Há quem diga que tudo isso deveria ser ensinado apenas na pós-graduação. Será? O Direito Digital é a evolução do próprio direito e permeia todas as suas disciplinas de modo transversal. Mas, mesmo em uma especialização, por que estes temas são mais bem tratados nas faculdades de tecnologia e administração do que nas jurídicas?

Quando a sociedade muda, o Direito também deve mudar, evoluir. Estamos vivendo a terceira grande revolução da humanidade, em que há uma completa transformação no modelo de riqueza, agora baseado nos ativos intangíveis, e nos valores e regras estabelecidas para reger as relações socioeconômicas, onde fazer um vírus ou mesmo praticar um furto de dados com uso do recurso de "CTRL C CTRL V" tornam-se condutas que precisam ser tratadas.

Esse descompasso na formação mais completa de profissionais que sejam estrategistas jurídicos faz com que não seja plantada a semente nesta nova geração de que cabe a eles escrever as novas leis, as novas sentenças, os novos contratos e acordos entre as partes, mantendo o equilíbrio e harmonia do Estado de Direito, fazendo com que haja segurança jurídica das relações e evitando-se que as pessoas, desesperadas por não serem atendidas por um Ordenamento mais bem preparado, acabem por buscar "fazer justiça com o próprio mouse".

Finalmente, a sociedade digital exige que os profissionais do Direito deixem de lado algumas rivalidades acadêmicas para discutirem conjuntamente paradigmas como ordenamento, legitimidade e segurança no âmbito de uma sociedade globalizada, convergente, digital e em constante mudança. É essa postura que o mercado vai cobrar. É esta a nova postura que os profissionais devem adotar para poder atuar no âmbito de uma sociedade digital.



Referências

- ABAR, Associação Brasileira de Arbitragem. *Regulamento*. 1999.
- ABREU, Fabíola Carolina Lisboa Cammarota de. *ISS X ICMS*, página da *web* [<http://www.cbeji.com.br/artigos/icmsXiss.htm>]. Acesso em: 7 jan. 2001 e 8 mar. 2006.
- ACQUAVIVA, Marcus Cláudio. *Dicionário jurídico brasileiro*. São Paulo: Jurídica Brasileira, 2000.
- AITH, Marcio. Invasão de privacidade. *Folha de S. Paulo*, 7 out. 2001, p. A-17.
- ALBERTANI, Luciane Jardim; LABER, Eduardo; PEREIRA, Pedro. *Internet e proteção legal à privacidade*, página da *web* [<http://www.redebrasil.inf.br/0artigos/internet.html>]. Acesso em: 8 mar. 2006.
- ALMEIDA, José Carlos de Araújo. *Manual de informática jurídica e direito da informática*. Rio de Janeiro: Forense, 2005.
- AMORIM, Divino Marcos de Melo. *Internet Brasil — Regulamentação estatal e órgãos reguladores — provedores de acesso ou informações e sua responsabilidade legal — Aplicabilidade do Código de Defesa do Consumidor*, página da *web* [<http://www.cbeji.com.br/artigos/artdivino06082001.htm>]. Acesso em: 8 mar. 2006 e 6 ago. 2001.
- ANDRADE, Paulo Gustavo Sampaio. *A importância da informática para o profissional do Direito*, página da *web* [<http://jus2.uol.com.br/doutrina/texto.asp?id=1758>]. Acesso em: 8 mar. 2006.
- ANDREATO, Danilo. *Direitos de personalidade e Internet*, página da *web* [<http://jus2.uol.com.br/doutrina/texto.asp?id=1983>]. Acesso em: 8 mar. 2006.
- ANUÁRIO Brasileiro de 2009. *Meios eletrônicos de pagamento*. São Paulo: ELAP, 2009.
- APRILE, Jurema. Sistema facilita a pesquisa no Código de Processo Civil. *Gazeta Mercantil*, 27/28 out. 2001, p. 2.

- ARAS, Vladimir. *Crimes de informática. Uma nova criminalidade*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2250]. Acesso em: 8 mar. 2006.
- ARDEN, Paul. *Tudo o que você pensa, pense ao contrário*. Rio de Janeiro: Intrínseca, 2008.
- ARRUDA, Hélio Mário de. *Ação e interação. Os debates e as pesquisas jurídicas na Internet*, página da web [http://www.ambito-juridico.com.br/aj/int0010b.htm]. Acesso em: 8 mar. 2006.
- ARRUDA JÚNIOR, Itamar. *O Código do Consumidor e a Internet. Quando aplicar?*, página da web [http://www.ambito-juridico.com.br/aj/dconsu0037.htm]. Acesso em: 8 mar. 2006.
- . *Documentos eletrônicos, autoridades certificadoras e legislação aplicável*, página da web [http://www.ambito-juridico.com.br/aj/int0010c.htm]. Acesso em: 8 mar. 2006.
- . *Injúria e difamação em meio virtual. Da teoria à prática*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=286]. Acesso em: 8 mar. 2006.
- . *Considerações ao PL n. 1589/99*, página da web [http://www.ambito-juridico.com.br/aj/int0010d.htm]. Acesso em: 8 mar. 2006.
- ASCENSÃO, José de Oliveira. *Direito da Internet e da sociedade da informação*. Rio de Janeiro: Forense, 2002.
- ASFORA, Carla Romeiro. *Processo civil como sistema autopoietico e aplicação do direito cibernético*, página da web [http://www.infojus.com.br/area4/carlaasfora.htm]. Acesso em: 8 mar. 2006.
- ASSIS, Luiz Carlos. Virtual também tem que ser legal. *B2B Magazine*, p. 56.
- ATHENIENSE, Alexandre. *Autoaplicação do Código do Consumidor nas transações de bens corpóreos pelo comércio eletrônico na Internet*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=173]. Acesso em: 8 mar. 2006.
- . *Subsídios para o Judiciário enfrentar os litígios de direito de informática: licenciamento de softwares*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1791]. Acesso em: 8 mar. 2006.
- . *Advocacia e informática*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1754]. Acesso em: 8 mar. 2006.
- AUGUSTO, Regina. O “grande irmão” e a privacidade. *Revista Meio & Mensagem*, p. 6, 28 out. 2001.
- AZEVEDO, Álvaro Villaça. *Teoria geral das obrigações*. 9. ed. São Paulo: Revista dos Tribunais, 2001.
- BANDEIRA DE MELLO, Celso Antônio. *Curso de direito administrativo*. 29. ed. São Paulo: Malheiros, 2012.
- BAPTISTA, Luiz Olavo. *Novas fronteiras do direito na informática e telemática*. São Paulo: Saraiva, 2001.
- . *Comércio eletrônico: uma visão do direito*. *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 94, p. 83-100, 1999.
- BARALDI, Paulo. *Gerenciamento de riscos*. Rio de Janeiro: Campus, 2004.
- BARBAGALO, Érica Brandini. *Contratos eletrônicos: contratos formados por meio de redes de computadores: peculiaridades jurídicas da formação do vínculo*. São Paulo, 2000.
- BARBOSA, Leonardo Figueiredo. *Tributação virtual*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=209]. Acesso em: 8 mar. 2006.
- BARBOSA, Lúcio de Oliveira. *Duplicata virtual — aspectos controvertidos*. São Paulo: Memória Jurídica, 2004.
- BARRA, Marcello Cavalcanti. *O Leviatã eletrônico*. Florianópolis: Edusc, 2009.
- BARROS, Felipe Luiz Machado. *Dos contratos eletrônicos no direito brasileiro*, página da web [http://www.suigeneris.pro.br/direito_dci_contratos.htm]. Acesso em: 8 mar. 2006.
- BASSO, Maristela. *Prudência no comércio eletrônico*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1803]. Acesso em: 8 mar. 2006.
- BATISTA, Daniel. *Advogados virtuais*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1798]. Acesso em: 8 mar. 2006.
- BEAL, Andy; STAUSS, Judy. *Radically transparent — monitoring and managing reputation online*. Indianopolis: Sybex, 2008.
- BENZATTI, Eduardo. A educação e os educadores do futuro. Disponível em: http://www.dominiopublico.gov.br/pesquisa/DetalheobraForm.do?select_action=&co_obra=105128.
- BERTOZZI, Rodrigo D. *Como ter uma boa página jurídica na Internet*, página da web [http://www.jurua.com.br/outros_artigos/internet_pag.asp]. Acesso em: 8 mar. 2006.
- . *Internet e direito: processos em torno do direito virtual*, página da web [http://www.jurua.com.br/outros_artigos/internet_dir.asp]. Acesso em: 8 mar. 2006.
- . *Direito virtual: aplicações para o direito do futuro*, página da web [http://www.jurua.com.br/outros_artigos/dir_virtual.asp]. Acesso em: 8 mar. 2006.
- BRANCHER, Paulo Marcos Rodrigues. *Contrato de “software”*. Florianópolis: Visual Books, 2003.
- BRANCO, Fábio Gonçalves Castelo. *A incidência do ICMS sobre os serviços de comunicação prestados pelos provedores de acesso à Internet*, página da web [http://150.162.138.14/arquivos/a_incidencia_do_ICMS_sobreSCPPAI.htm]. Acesso em: 8 mar. 2006.
- BRASIL, Angela Bittencourt. *Assinatura digital*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1782]. Acesso em: 8 mar. 2006.
- . *Difamação e injúria na web*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2153]. Acesso em: 8 mar. 2006.
- . *Assinatura digital não é assinatura formal*, página da web [http://www.ambito-juridico.com.br/aj/int0008.htm]. Acesso em: 8 mar. 2006.
- . *Petição através de e-mail*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=177]. Acesso em: 8 mar. 2006.

- . *Contratos virtuais*, página da web [http://www.advogado.com/internet/zip/contrato.htm]. Acesso em: 8 mar. 2006.
- . *Incoerência: lei anti-spam americana o torna legal*, página da web [http://www.cbeji.com.br/artigos/artang05%20-%2004062001.htm]. Acesso em: 8 mar. 2006.
- . *Pedofilia ou arte — a difícil fronteira*, página da web [http://www.widebiz.com.br/gente/angela/pedofiliarte.html]. Acesso em: 8 mar. 2006.
- . *Aplicação do Código do Consumidor na Internet*, página da web [http://www.ambito-juridico.com.br/aj/dconsu0024.htm]. Acesso em: 8 mar. 2006.
- . *Contrato virtual de empreitada*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1797]. Acesso em: 8 mar. 2006.
- . *Congresso sobre spams*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=191]. Acesso em: 8 mar. 2006.
- . *Empresas pontocom e seus advogados*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=224]. Acesso em: 8 mar. 2006.
- . *O documento físico e o documento eletrônico*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1781]. Acesso em: 8 mar. 2006.
- . *O sonho utópico de uma rede sem fronteiras*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2326]. Acesso em: 8 mar. 2006.
- . *Crimes de computador*, página da web [http://www.advogado.com/internet/zip/crimesdecomputador.htm]. Acesso em: 8 mar. 2006.
- BRASILIANO, Antonio Celso Ribeiro. *A insegurança nas redes empresariais*. São Paulo: Sicurezza, 2002.
- BRUNO, Gilberto Marques. *A disputa da fatia da arrecadação tributária na Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1968]. Acesso em: 8 mar. 2006.
- . *A rede mundial de computadores e a guerra fiscal brasileira na disputa pela arrecadação tributária*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2336]. Acesso em: 8 mar. 2006.
- . *Considerações sobre a criação da infraestrutura de chaves públicas brasileira e seu comitê gestor*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2310]. Acesso em: 8 mar. 2006.
- . *Considerações sobre os direitos autorais no "www". A proteção das criações do espírito e a necessidade de registro como meio de prova em casos de publicação*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2173]. Acesso em: 8 mar. 2006.
- . *Algumas considerações sobre a questão da validade, eficácia e valor probatório dos documentos eletrônicos e da assinatura digital*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2174]. Acesso em: 8 mar. 2006.
- . *O sigilo de dados e a privacidade on line — Anteprojeto de Lei do Comércio Eletrônico*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=256]. Acesso em: 8 mar. 2006.
- . *A Justiça Federal de São Paulo no ciberespaço — nasce a figura do processo virtual*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2175], 17.09.2001. Acesso em: 8 mar. 2006.

- . *As relações do "business to consumer" (B2C) no âmbito do "e-commerce"*, página da web [http://jus2.uol.com.br/DOCTRINA/texto.asp?id=2319]. Acesso em: 8 mar. 2006.
- BRUNO, Fabio de Barros. *E-Commerce e o direito de arrependimento*. Disponível em: <http://www.publicadireito.com.br/conpedi/manaus/arquivos/Anais/sao_paulo/2335.pdf>. Acesso em: 3 out. 2011.
- BRUNO, Marcos Gomes da Silva. *Aspectos jurídicos dos contratos eletrônicos*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2196]. Acesso em: 8 mar. 2006.
- BRUZOS, Odair. *O Pontocom é mais embaixo*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=197]. Acesso em: 8 mar. 2006.
- CABRAL, Antônio Carlos. *O contrato eletrônico*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=248]. Acesso em: 8 mar. 2006.
- CALVERT, Gene. *Gerência de alta tensão e de altos riscos*. São Paulo: Makron Books, 1999.
- CAMMAROTA, Fabíola. *ISS x ICMS*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=192]. Acesso em: 8 mar. 2006.
- CAMPOS, André L. N. *Sistema de segurança da informação*. Florianópolis: Visual Books, 2006.
- CANÇADO, Patricia. Um fórum virtual. *Revista Forbes Brasil*, 10 out. 2001.
- CARNEIRO, Guilherme de Carvalho. *Direitos autorais na era digital*, página da web [http://busclegis.cj.ufsc.br/arquivos/m10-DireitosAED.pdf]. Acesso em: 8 mar. 2006.
- CARVALHO, Ivan Lira de. *Crimes na Internet. Há como puni-los*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2081]. Acesso em: 8 mar. 2006.
- CASSEB, Rodney. Defesa do consumidor depois da Internet. *Gazeta Mercantil*, 27/28 out. 2001, p. A-2.
- CASTELLS, Manuel. *A galáxia da Internet*. Rio de Janeiro: Jorge Zahar, 2003.
- CASTRO, Aldemario Araujo. *Os meios eletrônicos e a tributação*, página da web [http://www.ambito-juridico.com.br/aj/dtrib0013.htm]. Acesso em: 8 mar. 2006.
- . *O documento eletrônico e a assinatura digital (uma visão geral)*, página da web [http://jus2.uol.com.br/DOCTRINA/texto.asp?id=2632]. Acesso em: 8 mar. 2006.
- . *A PGFN e a Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1814]. Acesso em: 8 mar. 2006.
- . *O sistema de pagamento on-line de débitos inscritos em dívida ativa da União: um marco na prestação de serviços ao contribuinte*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1815]. Acesso em: 8 mar. 2006.
- . *Validade jurídica de documentos eletrônicos. Considerações sobre o projeto de lei apresentado pelo Governo Federal*, página da web [http://www.ambito-juridico.com.br/aj/int0010.htm]. Acesso em: 8 mar. 2006.

- CASTRO, Carla Rodrigues Araújo de. *Impunidade na Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2327]. Acesso em: 8 mar. 2006.
- CASTRO, Clarice Marinho Martins de. *Nome de domínio na Internet e legislação de marcas*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1778]. Acesso em: 8 mar. 2006.
- CAVALCANTI, Sérgio. *A segurança no mundo virtual*, página da web [http://www.infojus.com.br/area1/sergiocavalcanti.htm]. Acesso em: 8 mar. 2006.
- CERQUEIRA, Tarcisio Queiroz. *O direito do ciberespaço*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1774]. Acesso em: 8 mar. 2006.
- . *Bug do ano 2000: limites da responsabilidade do fornecedor de software*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1823]. Acesso em: 8 mar. 2006.
- . *A regulamentação da Internet no Brasil*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1769]. Acesso em: 8 mar. 2006.
- CHRISTOVÃO, Daniela. AOL obtém reconhecimento de marca notória pelo INPI. *Valor*, 25 set. 2001.
- COIMBRA, Márcio Chalegre. *Direito de resposta e Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1775]. Acesso em: 8 mar. 2006.
- . *A inviolabilidade dos e-mails*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1787]. Acesso em: 8 mar. 2006.
- COLOMBO, Daniel Gama; Kung, Angela Fan Chi; Nunes, Esther Donio Bellegarde. *Spam e a legislação brasileira*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=261]. Acesso em: 8 mar. 2006.
- CONNELL, Andy. *Digital convergence*. Algis, 1995.
- CORRÊA, Gustavo Testa. *Responsabilidade na Internet: quem responde por crimes cometidos na rede?*, página da web [http://conjur.estadao.com.br/static/text/21474,1]. Acesso em: 8 mar. 2006.
- . *A lei e o comércio eletrônico*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1802]. Acesso em: 8 mar. 2006.
- . *Aspectos jurídicos da Internet*. São Paulo: Saraiva, 2000.
- CORRÊA, Lucia Helena. Brasil, um sonho intenso e eletrônico. *B2B Magazine*, maio 2001, p. 46.
- CORRÊA, Tatiana Machado. *Popularização da Internet, relações de consumo e sua proteção pelo direito*, página da web [http://jus2.uol.com.br/DOCTRINA/texto.asp?id=1800], 07.2000. Acesso em: 8 mar. 2006.
- CORREIA, Miguel Pupo. *Sociedade de informação e o direito: a assinatura digital*, página da web [http://www.advogado.com/internet/zip/assinatu.htm]. Acesso em: 8 mar. 2006.
- COSTA, Angelo Augusto. Uso da arbitragem chega a novos mercados. *Gazeta Mercantil*, 17 jul. 2000.

- COSTA, Luciana Borges da. *Comércio eletrônico — A validade jurídica dos contratos*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=179]. Acesso em: 8 mar. 2006.
- COSTA, Marco Aurélio Rodrigues da. *Crimes de informática*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1826]. Acesso em: 8 mar. 2006.
- COSTA, Marcos da; Marcacini, Augusto Tavares Rosa. *A urgência e relevância em violentar a Internet Brasileira*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2291]. Acesso em: 8 mar. 2006.
- . *O apagão do comércio eletrônico no Brasil*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2284]. Acesso em: 8 mar. 2006.
- CREMADES, Javier. *Micropoder — a força do cidadão na era digital*. São Paulo: Editora SENAC, 2009.
- CRONKHITE, Cathy; MCCULLOUGH, Jack. *Hackers: acesso negado*. Rio de Janeiro: Campus, 2001.
- DAOUN, Alexandre Jean. *Os novos crimes de informática*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1827]. Acesso em: 8 mar. 2006.
- . *Adulterio virtual*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2564]. Acesso em: 8 mar. 2006.
- DARRIGRANDI, Isabel; VASCONCELOS, Carlos. Despachante público. *América Economia*, 16 ago. 2001.
- DAUD, Pedro Victório. *Incidência tributária nas operações realizadas pela Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1812]. Acesso em: 8 mar. 2006.
- DAWEL, George. *A segurança da informação nas empresas*. Rio de Janeiro: Ciência Moderna, 2005.
- DE LUCCA, Newton. Contratos pela internet e via computador — requisitos de celebração, validade e eficácia: legislação aplicável. *Revista do Tribunal Regional Federal da 3ª Região*, São Paulo, n. 33, p. 20-37, jan./mar.1998.
- . *Aspectos jurídicos da contratação informática e telemática*. São Paulo: Saraiva, 2003.
- . *Direito & Internet*. São Paulo: Quartier Latin, 2008. v. II.
- DEITEL. *"E-business" e "e-commerce" para administradores*. São Paulo: Pearson Education, 2004.
- DELPUPPO, Poliana Moreira. *O direito do consumidor na era do comércio eletrônico*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=236]. Acesso em: 8 mar. 2006.
- DIAS, Cláudio. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000.
- DOMENEGHETTI, Daniel; MEIR, Roberto. *Ativos intangíveis — o real valor das empresas*. Rio de Janeiro: Campus, 2009.

- DUARTE, Fernanda et al. (coord.). *Os direitos à honra e à imagem pelo Supremo Tribunal Federal*. Rio de Janeiro: Renovar, 2006.
- ELIAS, Paulo Sá. *Vínculo contratual e a Internet*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=183]. Acesso em: 8 mar. 2006.
- . *A questão da reserva legal no direito penal e as condutas lesivas na área da informática e da tecnologia*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2038]. Acesso em: 8 mar. 2006.
- . *O documento eletrônico, a criptografia e o direito*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2073]. Acesso em: 8 mar. 2006.
- . *Triangulação no acesso à Internet. Aspectos positivos e negativos*, página da web [http://jus2.uol.com.br/DOCTRINA/texto.asp?id=2549]. Acesso em: 8 mar. 2006.
- . *Contratos eletrônicos bancários*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2674]. Acesso em: 8 mar. 2006.
- . *Alguns aspectos da informática e suas consequências no direito*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1762]. Acesso em: 8 mar. 2006.
- . *Ética na advocacia*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=193]. Acesso em: 8 mar. 2006.
- . *A tecnologia e o direito — Juristas não devem temer situações trazidas pela Web*, página da web [http://conjur.estadao.com.br/static/text/28465,1]. Acesso em: 8 mar. 2006.
- . *A Lei pode ser mais sábia que o legislador*, página da web [http://www.infojus.com.br/webnews/noticia.php?id_noticia=1268&]. Acesso em: 8 mar. 2006.
- . *A tecnologia e o direito no século XXI*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2099]. Acesso em: 8 mar. 2006.
- . *A tecnologia e o direito no século XXI: nova abordagem*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2547]. Acesso em: 8 mar. 2006.
- . *Contratos eletrônicos — e a formação do vínculo*. São Paulo: Lex Editora, 2008.
- . *Breves considerações sobre a formação do vínculo contratual e a Internet*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=183]. Acesso em: 8 mar. 2006.
- ERICKSON, Jon. *Hacking*. São Paulo: Digerati Books, 2009.
- ETCHEVERRY, Carlos Alberto. *O bug do milênio e o Direito*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1824]. Acesso em: 7 mar. 2006.
- FERRER, Florência. *E-Government: o governo eletrônico no Brasil*. São Paulo: Saraiva, 2004.
- FERREIRA, Ana Amelia Menna Barreto de Castro. *Inform@ção e priv@cidade*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=282]. Acesso em: 7 mar. 2006.

- . *Tributação ponto com*, página da web [http://www.ambito-juridico.com.br/aj/int0010g.htm]. Acesso em: 7 mar. 2006.
- . *Tributação do livro eletrônico*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=188]. Acesso em: 7 mar. 2006.
- . *e-Cartórios*, página da web [http://www.ambito-juridico.com.br/aj/int0010e.htm]. Acesso em: 7 mar. 2006.
- . *Tributação do comércio eletrônico*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=233]. Acesso em: 7 mar. 2006.
- . *Efeito dominó na tributação dos provedores de acesso*, página da web [http://www.ambito-juridico.com.br/aj/dtrib0027.htm]. Acesso em: 7 mar. 2006.
- . *Colcha de retalhos da MP 2.200*, página da web [http://www.cbeji.com.br/artigos/artanaamelia17092001.htm]. Acesso em: 7 mar. 2006.
- FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de segurança da informação*. Rio de Janeiro: Ciência Moderna, 2008.
- FERREIRA, Marcelo Ferraz. *A lei, o consumidor e o cyberspace*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1799]. Acesso em: 7 mar. 2006.
- FERREIRA, Paulo Roberto G. *A assinatura digital é assinatura formal*, página da web [http://www.cbeji.com.br/artigos/artcartorio_assformal.htm]. Acesso em: 7 mar. 2006.
- . *Cartórios na nova economia*, página da web [http://www.direitoemdebate.net/art_novaeco.html]. Acesso em: 7 mar. 2006.
- FERREIRA, Robson. *Textos acadêmicos*, dez. 2001.
- FERREIRA, Solon Angelim de Alencar. *A aplicação do Código de Defesa do Consumidor às mensagens publicitárias não solicitadas recebidas através da Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2575]. Acesso em: 7 mar. 2006.
- FIGUEIREDO, Odail. *Formato Digital deve Promover Transparência*. *Gazeta Mercantil*, 17 out. 2000.
- FINATI, Claudio Roberto. *Relações de trabalho na era da informática*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=187]. Acesso em: 7 mar. 2006.
- FINKLSTEIN, Maria Eugênia Reis. *Aspectos jurídicos do comércio eletrônico*. Porto Alegre: Síntese, 2004.
- FLEMING, Gil Messias. *Pirataria: uma abordagem social*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1042]. Acesso em: 7 mar. 2006.
- FONTANARI FILHO, Pedro. *Particular*, página da web [http://www.advogado.com/internet/zip/privado.htm]. Acesso em: 7 mar. 2006.
- FONTES, Edson. *Praticando a segurança da informação*. Rio de Janeiro: Brasport, 2008.
- FRANCO, Antonio Celso Pinheiro. *Prática de contratos e instrumentos particulares*. São Paulo: Revista dos Tribunais, 2005.

- FREITAS, Andrey Rodrigues de. *Perícia forense aplicada à informática*. Rio de Janeiro: Brasport, 2006.
- FRIGERI, Marcia Regina. *Responsabilidade civil dos estabelecimentos bancários*. Rio de Janeiro: Forense, 1997.
- GANDELMAN, Henrique. *De Gutenberg à Internet: direitos autorais na era digital*. 4. ed. Rio de Janeiro: Record, 2001.
- GANDELMAN, Silvia Regina Dain. *A proteção do consumidor na Internet*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=195]. Acesso em: 7 mar. 2006.
- GIL, Antônio Loureiro. *Fraudes informatizadas*. 2. ed. São Paulo: Atlas, 1999.
- GLATER, Jonathan D. *Ideas & trends*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=194]. Acesso em: 7 mar. 2006.
- GOLDEN, Thomas W.; SKALAK, Steven L.; Clayton, Mona M. *A guide to forensic accounting investigation*. New Jersey: John Wiley & Sons, 2005.
- GONÇALVES, Sérgio Ricardo M. *E-mail x empregados: é legal o monitoramento pela empresa?*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=280]. Acesso em: 7 mar. 2006.
- . *O "recall" e a verdadeira proteção do consumidor*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=264]. Acesso em: 7 mar. 2006.
- . *O Direito de arrependimento nas compras pela Internet*, página da web [http://www.cbeji.com.br/artigos/artsergiogolcalves/artsergiogoncalves26112001.htm]. Acesso em: 7 mar. 2006.
- . *O Windows XP, a pirataria e os direitos dos consumidores*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2422]. Acesso em: 7 mar. 2006.
- GOUVÊA, Sandra. *O direito na era digital: crimes praticados por meio da informática*. Rio de Janeiro: Mauad, 1997.
- GRECO, Marco Aurélio. *Internet e direito*. 2. ed., rev. e aum. São Paulo: Dialética, 2000.
- GRECO, Marco Aurélio et al. *Direito e Internet — relações jurídicas na sociedade informatizada*. São Paulo: Revista dos Tribunais, 2001.
- GUBERT, Pablo Andrez Pinheiro. *O registro de domínio e o alcance da marca registrada*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1779]. Acesso em: 7 mar. 2006.
- GUEIROS JÚNIOR, Nehemias. *A revolução do MP3*, página da web [http://150.162.138.14/arquivos/A_revolu%C3%A7ao_do_MP3.htm]. Acesso em: 10 mar. 2006.
- . *Os sons ameaçadores da grande rede*, página da web [http://www.juristaonline.com.br/artigos/arquivos/informatica_juridica/os_sons.htm]. Acesso em: 10 mar. 2006.

- GUSMÃO, Cláudia Regina. *Incidência do ICMS sobre o serviço de comunicação por provedor de Internet*. Parecer PGFN, página da web [http://www.geocities.com/Athens/Olympus/7393/icmsinternet.htm]. Acesso em: 10 mar. 2006.
- HEIJDEN, Kees Van Der. *Planejamentos de cenários — a arte da conversação estratégica*. Porto Alegre: Bookman, 2004.
- HUNTINGTON, Samuel P. *The Clash of Civilization*. Touchstone/ Simon & Schuster, 1999.
- JENKINS, Henry. *Cultura da convergência*. São Paulo: Aleph, 2008.
- JESUS, Damásio E. de. *Eu e o computador*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1755]. Acesso em: 10 mar. 2006.
- JOHNSON, Steven. *Computação forense*. Rio de Janeiro: Jorge Zahar, 2003.
- JOLIBERT, Josette. *Além dos muros da escola*. Porto Alegre: Artmed, 2006.
- KAMINSKI, Omar. *A Internet e o ciberespaço*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1770]. Acesso em: 10 mar. 2006.
- . *A regulamentação da Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1768]. Acesso em: 10 mar. 2006.
- . *A Internet e os bancos de dados*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=278]. Acesso em: 10 mar. 2006.
- . *Jurisdição na Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1834]. Acesso em: 10 mar. 2006.
- . *Um "screenshot" dos nomes de domínio no Brasil*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2259]. Acesso em: 10 mar. 2006.
- KLAVA, Luis Fernando. Menos papel com os documentos digitais. *Gazeta Mercantil*, 25 out. 2000.
- KOEPSSELL, David R. *A filosofia, a lei e o futuro da propriedade intelectual*. São Paulo: Madras, 2005.
- LANDY, Gene K. *The software developer's and marketers legal companies*. Massachusetts: Addison Wesley, 1993.
- LIMA, Arnaldo Siqueira de. *A pirataria e a atribuição para investigar*, página da web [http://www.neofito.com.br/artigos/art01/juridi74.htm]. Acesso em: 10 mar. 2006.
- LIMA, George Marmelstein. *A reprodução não autorizada de obras literárias na Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1792]. Acesso em: 10 mar. 2006.
- LIMA JR., Carlos Daniel Vaz de. *O sigilo do cadastro de clientes dos provedores de acesso à Internet*, página da web [http://idgb.com.br/modules.php?name=News&file=article&sid=44]. Acesso em: 10 mar. 2006.
- LIMA NETO, José Henrique Barbosa Moreira. *Alguns aspectos jurídicos da Internet no Brasil*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1772]. Acesso em: 10 mar. 2006.

- . *Alguns comentários sobre o registro de domain no Brasil*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1777]. Acesso em: 10 mar. 2006.
- . *Aspectos jurídicos do documento eletrônico*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1780]. Acesso em: 10 mar. 2006.
- . *Violação de direitos autorais na Internet*, página da web [http://www.juridica.com.br/fra_textos_atuali.asp?CodArtigo=36]. Acesso em: 10 mar. 2006.
- LIMEIRA, Tania M. Vidigal. *"E-marketing" — o marketing na Internet com casos brasileiros*. São Paulo: Saraiva, 2003.
- LÓPEZ, Valentino Cornejo; Paiva, Mário Antônio Lobato de. *O documento, a firma e o notário eletrônico*, página da web [http://www.ambito-juridico.com.br/aj/int0010k.htm]. Acesso em: 10 mar. 2006.
- LUCENA NETO, Cláudio de. *A formação do profissional de direito na tecnologia da Informação*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1759]. Acesso em: 10 mar. 2006.
- LUNA FILHO, Eury Pereira. *Internet no Brasil e o Direito no ciberespaço*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1773]. Acesso em: 10 mar. 2006.
- . *Notas sobre a Lei de Proteção a Programas de Computador*, página da web [http://www.infojus.com.br/area1/euryluna4.html]. Acesso em: 10 mar. 2006.
- . *Limites constitucionais à tributação na Internet*, página da web [http://www.infojus.com.br/area1/euryluna10.htm]. Acesso em: 10 mar. 2006.
- MACEDO, Néstor Adolfo Mamani. *O comércio eletrônico na Internet é uma realidade no Brasil*, página da web [http://www.dcc.ufba.br/~frieda/mat159/comrcio.htm]. Acesso em: 10 mar. 2006.
- . *O contrato eletrônico de e-mail*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=284]. Acesso em: 10 mar. 2006.
- MACHADO, Hugo de Brito; Machado Segundo, Hugo de Brito. *Imunidade tributária do livro eletrônico*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1809]. Acesso em: 10 mar. 2006.
- MACIEL, Marco. *Avanço digital e hiato social*, *O Estado de S. Paulo*, 16 jul. 2001, p. 17-2.
- . *A arbitragem na solução das controvérsias*, *Jornal de Brasília*, 13 abr. 1999, p. 6-A.
- MADALENA, Pedro; Oliveira, Álvaro Borges de. *O Judiciário dispondo dos avanços da informática*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2553]. Acesso em: 10 mar. 2006.
- MAGNAVITA, Mônica. Múltis adotam o juízo arbitral em seus contratos. *Gazeta Mercantil*, 19 out. 2000.
- MANUCCI, Daniel Diniz. *Código de Defesa do Consumidor x Internet*, página da web [http://www.redebrasil.inf.br/0artigos/procon.htm], 07.2000. Acesso em: 10 mar. 2006.

- MARANO, Lina. *O spam e o Direito*, página da web [http://www.neofito.com.br/artigos/art01/inform17.htm]. Acesso em: 10 mar. 2006.
- MARCACINI, Augusto Tavares Rosa. *O documento eletrônico como meio de prova*, página da web [http://www.advogado.com/internet/zip/tavares.htm]. Acesso em: 10 mar. 2006.
- MARQUES, Renata Ribeiro. *Aspectos do comércio eletrônico aplicados ao direito brasileiro*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2467]. Acesso em: 10 mar. 2006.
- MARTINELLI, João Paulo Orsini. *Aspectos relevantes da criminalidade na Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1829]. Acesso em: 10 mar. 2006.
- MARTINS, Henrique de Faria. *Assinaturas eletrônicas — o primeiro passo para o desenvolvimento do comércio eletrônico?*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=171]. Acesso em: 10 mar. 2006.
- . *E-mail de funcionários pode ser violado?*, página da web [http://www.cbeji.com.br/artigos/artviolacaodeemails.htm]. Acesso em: 10 mar. 2006.
- MARTINS, Ives Gandra da Silva. *A Internet e as questões tributárias: ISS ou ICMS?*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2562]. Acesso em: 10 mar. 2006.
- . *A imunidade do livro eletrônico*, página da web [http://150.162.138.14/arquivos/A_imunidade_do_livro_eletronico.html]. Acesso em: 14 mar. 2006.
- MARZOCHI, Marcelo de Luca. *Direito.br — aspectos jurídicos da Internet no Brasil*. São Paulo: LTr, 2001.
- . *Pornografia na Internet*, página da web [http://www.direitonet.com.br/textos/x/51/11/51/]. Acesso em: 14 mar. 2006.
- MATA, Brenno Guimarães Alves da. *Análise e tendências do cenário jurídico atual na Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1771]. Acesso em: 14 mar. 2006.
- MATEUCCI, Carlos Roberto Fornes. *Privacidade e e-mail*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=276]. Acesso em: 14 mar. 2006.
- MATTE, Maurício. *Internet e comércio eletrônico — aplicabilidade do Código de Defesa do Consumidor nos Contratos de e-Commerce*. São Paulo: LTr, 2001.
- MELLO, Eduardo Piza Gomes de. *A Receita Federal e seus cartórios cibernéticos*, página da web [http://www.advogado.com/internet/zip/recfederal.htm]. Acesso em: 14 mar. 2006.
- MENDES, Murillo; ATTUCH, Leonardo. *Quebra de contrato — o pesadelo dos brasileiros*. Belo Horizonte: Folium, 2008.
- MENSAGEM indesejada — empresa indeniza internauta por envio de spam. *Revista Consultor Jurídico*, 28 jun. 2001.

- MENSAGENS indesejadas — yahoo do Brasil é processado por engenheiro no RS. *Revista Consultor Jurídico*, 14 set. 2001.
- MILLEO, Maritza Fabiane; Saldan, Eliane. *O monitoramento e interceptação de e-mail*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=285]. Acesso em: 14 mar. 2006.
- MIRANDA, Marcelo Baeta. *Abordagem dinâmica aos crimes via Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1828]. Acesso em: 14 mar. 2006.
- MONTEIRO, Fernanda. *Informática para Advogados*, página da web [http://www.datavenia.net/opiniao/2001/Informatica-para-Advogados.htm]. Acesso em: 14 mar. 2006.
- MORON, Fernanda de A. Pernambuco. *A Internet e o direito*, página da web [http://www.juridica.com.br/fra_textos_atuali.asp?CodArtigo=23]. Acesso em: 14 mar. 2006.
- MOTTA, Carlos. *Internet — um novo caminho ou um caminho novo?*, página da web [http://www.advogado.com/internet/zip/internet.htm]. Acesso em: 14 mar. 2006.
- . *A responsabilidade do Web Designer em casos de invasão de web sites*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=277]. Acesso em: 14 mar. 2006.
- MURRAY, Brian H. *Defending the brand*. Amacom, 2004.
- NEVES, Carvalho. *Direitos autorais e citação de documentos eletrônicos da Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1793]. Acesso em: 14 mar. 2006.
- NG, Reynaldo. *Forense computacional corporativa*. Rio de Janeiro: Brasport, 2007.
- NINA, Alexandre de Mendes. *A Internet e a liberdade de expressão*, página da web [http://150.162.138.14/arquivos/A_Internet_e_a_liberdade_de_expressao.html]. Acesso em: 14 mar. 2006.
- NOGUEIRA, Fernando Célio de Brito. *Violação de e-mail é crime?*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1789]. Acesso em: 14 mar. 2006.
- O'CONNOR, John; FELT, Mark. *A vida do garganta profunda*. Rio de Janeiro: Record, 2009.
- OLIVEIRA, Alirio Araújo de. *Os crimes na informática, deficiências na legislação*, página da web [http://www.infojus.com.br/webnews/noticia.php?id_noticia=497&c]. Acesso em: 14 mar. 2006.
- OLIVEIRA, Celso. *Parecer a não incidência do ICMS e o ISS sobre a atividade de provedor de serviços Internet*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=214]. Acesso em: 14 mar. 2006.
- . *Informativo especial para as empresas provedoras de serviços Internet*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=225]. Acesso em: 14 mar. 2006.
- OLIVEIRA JÚNIOR, João Batista Caldeira de. *A Internet e os "novos" crimes virtuais. A fronteira cibernética*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2097], 05.2001. Acesso em: 14 mar. 2006.
- OLIVEIRA, Marcelo Ribeiro de. *A atividade notarial digital em face do Projeto de Lei 1.589/99*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1805]. Acesso em: 14 mar. 2006.
- OLIVEIRA, Yonne Dolacio de. A imunidade do art. 150, inciso VI, alínea d, da Constituição Federal abrange ou não o denominado livro eletrônico. In: Machado, Hugo de Brito (Coord.). *Imunidade tributária do livro eletrônico*. São Paulo: IOB, 1998.
- PAESANI, Liliane Minardi. *Direito e Internet*. São Paulo: Atlas, 2000. (Col. Temas Jurídicos).
- PAIVA, Mário Antônio Lobato de. *O impacto da informática no direito do trabalho*, página da web [http://www.ambito-juridico.com.br/aj/dtrab0052.htm]. Acesso em: 14 mar. 2006.
- . *A informatização da demissão*, página da web [http://www.ambito-juridico.com.br/aj/dtrab0035.htm]. Acesso em: 14 mar. 2006.
- . *A ciência do direito informático*, página da web [http://www.advogado.adv.br/artigos/2001/mlobatopaiva/direitoinformatica.htm]. Acesso em: 14 mar. 2006.
- . *O e-mail como instrumento de divulgação sindical*, página da web [http://www.ambito-juridico.com.br/aj/dtrab0050.htm]. Acesso em: 14 mar. 2006.
- PAIVA, Mário Antônio Lobato de; López, Valentino Cornejo. *O documento, a firma e o notário eletrônico*, página da web [http://www.ambito-juridico.com.br/aj/int0010k.htm]. Acesso em: 14 mar. 2006.
- PATERSON, Michael. *Decifradores de códigos*. São Paulo: Larousse do Brasil, 2009.
- PEIXOTO, Marco Aurélio Ventura. *Documentos eletrônicos: a desmaterialização dos títulos de crédito*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2361]. Acesso em: 14 mar. 2006.
- PEREIRA, Alexandre Libório Dias. *Comércio eletrônico na sociedade da informação: da segurança técnica à confiança jurídica*. Coimbra: Almedina, 1999.
- PEREIRA JÚNIOR, Álvaro. Lei reforça vigilância na Internet. *Folha de S. Paulo*, 7 out. 2001.
- PEREIRA, Marcelo Cardoso. *O sistema de proteção de dados pessoais frente ao uso da informática e o papel do direito de autodeterminação informativa. Especial referência ao ordenamento jurídico espanhol*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2266]. Acesso em: 14 mar. 2006.
- . *Breves considerações sobre direito informático e informática Jurídica*, página da web [http://www.ambito-juridico.com.br/aj/int0009c.htm]. Acesso em: 14 mar. 2006.
- PERENTY, Thomas J. *Digital defense*. Harvard: Harvard Business School Press, 2003.

- PERES, Tatiana. Margem de manobra. *Revista Forbes Brasil*, 10 out. 2001.
- PETERSEN FILHO, Antonio Oscar de Carvalho. *A nova Lei de Software*, página da web [http://www.infojus.com.br/area1/antonio.htm]. Acesso em: 14 mar. 2006.
- PIMENTA, Luiz Edgard Montauray. *O conflito de nomes de domínio e marcas à luz das decisões judiciais no Brasil*, página da web [http://www.cbeji.com.br/artigos/nomes%20de%20dominio.htm]. Acesso em: 14 mar. 2006.
- PIMENTEL, Alexandre Freire. *Do direito natural ao direito artificial*, página da web [http://www.infojus.com.br/area1/alex1.html]. Acesso em: 14 mar. 2006.
- PINHEIRO, Patricia Peck; BISSOLI, Leandro. *Eleições digitais* (audiolivro). São Paulo: Saraiva, 2010.
- PINHEIRO, Patricia Peck; SLEIMAN, Cristina Moraes. *Tudo o que precisa ouvir sobre direito digital no dia a dia*. São Paulo: Saraiva, 2008.
- PINHEIRO, Reginaldo César. *Os cybercrimes na esfera jurídica brasileira*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1830]. Acesso em: 14 mar. 2006.
- PINTO, Marcio Morena. *As relações jurídicas de consumo na era da economia digital*, página da web [http://www.alfa-redi.org/rdi-articulo.shtml?x=825]. Acesso em: 14 mar. 2006.
- . *O direito da Internet: O nascimento de um novo ramo jurídico*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2245]. Acesso em: 14 mar. 2006.
- PIRES, Leonardo Gurgel Carlos. *O e-mail e os aspectos probatórios no direito brasileiro*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1786]. Acesso em: 14 mar. 2006.
- PONTES, Marcelo. *E-Learning: Educação na velocidade da Internet*. *B2B Magazine*, maio 2001, p. 26.
- PRADO, Cláudio de Abreu; Passarelli, Marcos Vinícius. *An Overview of the relevant Brazilian tax issues in the Internet*, página da web [http://www.cbeji.com.br/br/us/novidades/artigos/main.asp?id=205]. Acesso em: 15 mar. 2006.
- PROMOTOR critica envio de mensagens indesejadas — lixo cibernético. *Revista Consultor Jurídico*, 11 set. 2001.
- RECTOR, Marcus. *Comércio eletrônico no Brasil*, página da web [http://150.162.138.14/arquivos/comercio_eletronico_no_brasil.htm]. Acesso em: 15 mar. 2006.
- RÊGO, Cláudio Andrade. *Cartórios eletrônicos e o exercício ilegal de profissão*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2420]. Acesso em: 15 mar. 2006.
- REINALDO FILHO, Demócrito. *O futuro da proteção intelectual na Internet*, página da web [http://www.infojus.com.br/webnews/noticia.php?id_noticia=215&]. Acesso em: 15 mar. 2006.
- . *A questão da validade jurídica dos atos negociais por meios eletrônicos*, página da web [http://www.infojus.com.br/area1/democritofilho13.htm]. Acesso em: 15 mar. 2006.

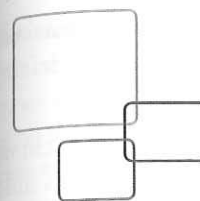
- . *A pedofilia na Internet e a atuação do FBI*, página da web [http://www.infojus.com.br/area1/democritofilho12.htm]. Acesso em: 15 mar. 2006.
- . *O homeschooling na era da Internet*, página da web [http://www.infojus.com.br/area1/democritofilho7.htm]. Acesso em: 15 mar. 2006.
- . *As comunidades virtuais*, página da web [http://www.infojus.com.br/area1/democritofilho6.html]. Acesso em: 15 mar. 2006.
- . *Tecnologias da informação: novas linguagens do conhecimento*, página da web [http://www.infojus.com.br/area1/democritofilho5.html]. Acesso em: 15 mar. 2006.
- . *Responsabilidade do provedor por mensagens difamatórias*, página da web [http://www.infojus.com.br/webnews/noticia.php?id_noticia=213&]. Acesso em: 15 mar. 2006.
- REYNOLDS, George. *Ethics in information technology*. Thomson Learning, 2007.
- REZENDE, Ana Paula de. *Utilizando a INTERNET em pesquisas jurídicas*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=186]. Acesso em: 15 mar. 2006.
- REZENDE, Pedro Antonio Dourado de. *2350 anos de retrocesso, na informática*, página da web [http://www.cic.unb.br/docentes/pedro/trabs/fust3.htm]. Acesso em: 15 mar. 2006.
- . *O silêncio que produz ruídos*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=279]. Acesso em: 15 mar. 2006.
- . *A ALCA e o cenário de Princeton*, página da web [http://www.cic.unb.br/docentes/pedro/trabs/Princeton.htm]. Acesso em: 15 mar. 2006.
- . *Totalitarismo digital*, página da web [http://www.cic.unb.br/docentes/pedro/trabs/ditadura.htm]. Acesso em: 15 mar. 2006.
- . *O Brasil fustigado*, página da web [http://www.cic.unb.br/docentes/pedro/trabs/fust2.htm]. Acesso em: 15 mar. 2006.
- . *Um pacote Xurpresa!*, página da web [http://www.cic.unb.br/docentes/pedro/trabs/Xurpresa.htm]. Acesso em: 15 mar. 2006.
- . *Palavras mágicas sobre entidades certificadoras, assinaturas eletrônicas e projetos de lei. Palestra Proferida no 1º Congresso Mineiro de Direito na Informática*, página da web [http://www.cic.unb.br/docentes/pedro/trabs/oab.htm]. Acesso em: 15 mar. 2006.
- . *Onde estão os verdadeiros crimes de informática?*, página da web [http://www.cic.unb.br/docentes/pedro/trabs/crimes.htm]. Acesso em: 15 mar. 2006.
- RIBAS, Sílvio. Livre informação para ganhar competitividade. *Gazeta Mercantil*, 25 out. 2000, p. A-5.
- RISO, Douglas Leme de. *Certificação eletrônica privada — uma nova atividade aos profissionais liberais?*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=180]. Acesso em: 15 mar. 2006.

- . *assinatur@eletronic@: certeza ou insegurança?*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=181]. Acesso em: 15 mar. 2006.
- . *Regulamentação da certificação eletrônica*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=242]. Acesso em: 15 mar. 2006.
- ROQUE, Sebastião José. *Arbitragem, a solução viável*. São Paulo: Ícone, 1997.
- ROSA, Antonio. Você já entendeu o t-Commerce?. *B2B Magazine*, maio 2001, p. 28.
- . A revolução da interatividade. *B2B Magazine*, jun. 2001, p. 34.
- ROSSI, Anamaria; SOMENZARI, Luciano. Nova Lei de Informática — volta ao formato original. *Gazeta Mercantil*, 25 out. 2000, p. A-10.
- ROSSI, Fernando Fonseca. *Ética na publicidade on line da advocacia*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1807]. Acesso em: 15 mar. 2006.
- SALDAN, Eliane; Cunha, Ellen Cristina. *Evasão fiscal através do e-commerce*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=245]. Acesso em: 15 mar. 2006.
- SANT'ANNA, Paulo Afonso de Souza. *Atenção, analfabets!*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1757]. Acesso em: 15 mar. 2006.
- SANT'ANNA, Paulo José. Privacidade em pauta. *Revista Meio & Mensagem*, 28 ago. 2000.
- SANTOLIM, Cesar Viterbo Matos. *Formação e eficácia probatória dos contratos por computador*. São Paulo: Saraiva, 1995.
- SANTOS, Cleber Mesquita dos. *Interceptação da comunicação em sistemas informáticos e telemáticos*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=176]. Acesso em: 15 mar. 2006.
- SANTOS, Fabiano Pereira dos. *Incidência tributária sobre operações comerciais envolvendo "software"*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2233]. Acesso em: 15 mar. 2006.
- SARAGIOTTO, Thiago Pélico. *Apontamentos acerca da tormentosa relação entre marca e domínio no Brasil*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2171]. Acesso em: 15 mar. 2006.
- SCHOUERI, Luís Eduardo. *Internet — o direito na era virtual*. São Paulo: Melhoramentos, 2000.
- SÊMOLA, Marcos. *Gestão da segurança da informação — uma visão executiva*. Rio de Janeiro: Campus, 2003.
- SIEBEL, Thomas M.; HOUSE, Pat. *Cyber Rules*. New York: Currency/Doubleday, 1999.
- SILVA JÚNIOR, Ronaldo Lemos et al. *Comércio eletrônico*. São Paulo: Revista dos Tribunais, 2001.
- SILVA, Antônio Everardo Nunes da. *Segurança da informação, vazamento de informações. As informações estão realmente seguras em sua empresa?* Rio de Janeiro: Ciência Moderna, 2011.

- SILVA, Mauro Marcelo de Lima e. *Ética na informática*, página da web [http://www.cbeji.com.br/artigos/artmauromarcelo10042001.htm]. Acesso em: 15 mar. 2006.
- SILVA NETO, Amaro Moraes e. *O e-mail como prova no direito brasileiro*, página da web [http://www.advogado.com/internet/zip/prova.htm]. Acesso em: 15 mar. 2006.
- . *O e-mail como prova no direito alienígena*, página da web [http://www.advogado.com/internet/zip/prova2.htm]. Acesso em: 15 mar. 2006.
- . *O spam e a legislação brasileira*, página da web [http://www.advogado.com/spam.htm]. Acesso em: 15 mar. 2006.
- . *O anonimato na Web*, página da web [http://www.advogado.com/internet/zip/anonimo.htm]. Acesso em: 15 mar. 2006.
- . *O direito e o espaço cibernético*, página da web [http://www.juridica.com.br/fra_textos_atuali.asp?CodArtigo=14]. Acesso em: 15 mar. 2006.
- . *A responsabilidade do webmaster decorrente da introdução de cookies*, página da web [http://www.cbeji.com.br/artigos/artam01.htm]. Acesso em: 15 mar. 2006.
- . *Provocação ao Ministério Público de São Paulo no sentido de serem apuradas as responsabilidades dos spammers brasileiros*, página da web [http://www.cbeji.com.br/jurisprudencia/spam1.htm]. Acesso em: 15 mar. 2006.
- . *Resgatemos os hackers*, página da web [http://jus2.uol.com.br/DOUTRINA/texto.asp?id=1831]. Acesso em: 15 mar. 2006.
- . *A transnacionalidade do ciberespaço*, página da web [http://www.advogado.com/zip/ciber-01.htm]. Acesso em: 15 mar. 2006.
- . *O domain name e a marca*, página da web [http://www.advogado.com/zip/ciber-02.htm]. Acesso em: 15 mar. 2006.
- . *Cookies, estes indigestos biscoitos...*, página da web [http://www.advogado.com/internet/zip/cookies.htm]. Acesso em: 15 mar. 2006.
- . *O Código do Consumidor e os softwares que nos são impostos*, página da web [http://www.advogado.com/internet/zip/con-ms.htm]. Acesso em: 15 mar. 2006.
- SILVA, Rosana Ribeiro da. *Contratos eletrônicos*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1794]. Acesso em: 15 mar. 2006.
- . *A viabilidade da prática de atos processuais via meios eletrônicos. Parágrafo único do art. 154 do 13º Anteprojeto de Reforma da Legislação Processual*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1806]. Acesso em: 15 mar. 2006.
- SILVERSTEIN, Barry. *Business-to-business Internet marketing*. 2. ed. Maximum Press, 2000.
- SINGH, Simon. *The Code Book. The science of secrecy from Ancient Egypt to Quantum Cryptography*. London: Anchor Books, 1999.
- SMITH, Richard E. *Internet cryptography*. Massachusetts: Addison Wesley, 1997.

- SOIBELMAN, Félix. *O direito e a informática*, página da web [http://www.advogado.com/analisis01.htm]. Acesso em: 15 mar. 2006.
- SOUZA, Carmen de Carvalho e. *Do Estado: uma análise de sua evolução e o papel inevitável da informática em seu processo de adequação aos tempos atuais*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1763]. Acesso em: 15 mar. 2006.
- SOUZA, Marcos Antonio Cardoso de. *Sigilo das mensagens eletrônicas dos funcionários de empresas e órgãos públicos*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1788]. Acesso em: 15 mar. 2006.
- . *A legislação e a Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1767]. Acesso em: 15 mar. 2006.
- SOUZA, Vinicius. Governo eletrônico atrai fornecedores. *Gazeta Mercantil*, 17 out. 2000.
- STACCHINI, Adriana d'Essen. Arbitragem e a resolução de conflitos. *Gazeta Mercantil*, 8 out. 2001.
- STREIT, Renata. *Às vezes, é melhor não fazer*, página da web [http://www.cbeji.com.br/artigos/artgilbertobruno08102001-3.htm]. Acesso em: 15 mar. 2006.
- STRINGHER, Ademar. *Aspectos legais da documentação em meios micrográficos digitais e eletrônicos*. São Paulo: Cenadem, 2003.
- STUBER, Walter D.; FRANCO, Ana Cristina. *Internet sob a óptica jurídica*, página da web [http://www.infojus.com.br/area1/waltereanafranco1.htm]. Acesso em: 15 mar. 2006.
- SZKLAROWSKY, Leon Frejda. *A informática e o mundo moderno*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1756]. Acesso em: 15 mar. 2006.
- TEIXEIRA, Rômulo José de Medeiros. *ICMS na operação mercantil com software*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1810]. Acesso em: 15 mar. 2006.
- TORRES FILHO, Pedro. *Implicações ético-jurídicas das novas tecnologias da informação*, página da web [http://www.infojus.com.br/area1/Pedro%20Torres.htm]. Acesso em: 15 mar. 2006.
- TRIPADALLI, Elídia. *Disciplina; tópicos de direito internacional privado para gestão empresarial*, página da web [http://cbeji.com.br/br/novidades/artigos/main.asp?id=239], 06.08.2001. Acesso em: 15 mar. 2006.
- TRUJILLO, Elcio. *O Mercosul e a documentação eletrônica*, página da web [http://www.advogado.com/zip/mercosul.htm]. Acesso em: 15 mar. 2006.
- TUCCI, José Rogério Cruz e. Eficácia probatória dos contratos celebrados pela Internet. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (Coords.). *Direito e Internet — Aspectos jurídicos relevantes*. Bauru: EDIPRO, 2000.
- TURBAN, Efrain; RAINER JR., R. Kelly; POTTER, Richard E. *Administração de tecnologia da informação*. Rio de Janeiro: Campus, 2005.

- VENCIGUERRA, Márcio; BOHONE, Flávia. Opção pela arbitragem deve ser lenta e mais atrativa aos estrangeiros. *Gazeta Mercantil*, 7 maio 2001.
- VIANNA, Túlio Lima. *Dos crimes por computador*, página da web [www.mundojuridico.adv.br/cgi-bin/upload/texto259.rtf]. Acesso em: 15 mar. 2006.
- VIDIGAL, Geraldo Facó. *Assinaturas digitais e certificação*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1784]. Acesso em: 15 mar. 2006.
- VOLPI NETO, Angelo. *Os "cartórios" do mundo*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=231]. Acesso em: 15 mar. 2006.
- WACHOWICZ, Marcos. *O programa de computador e sua proteção no Brasil*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=2530]. Acesso em: 15 mar. 2006.
- WESTERMAN, George; HUNTER, Richard. *O risco de TI — convertendo ameaças aos negócios em vantagens competitivas*. São Paulo: M. Books, 2008.
- WOLF, Karen Emilia Antoniazzi. *A possibilidade de incidência do ICMS nas operações da Internet*, página da web [http://jus2.uol.com.br/doutrina/texto.asp?id=1811]. Acesso em: 15 mar. 2006.
- ZAITZ, Daniela. *Direito & "know-how" — uso, transmissão e proteção dos conhecimentos técnico ou comercial*. Curitiba: Juruá, 2005.
- ZANCHI, Marta B.T. *A honra na imprensa*, página da web [http://150.162.138.14/arquivos/A_honra_na_imprensa_.html]. Acesso em: 15 mar. 2006.
- ZANETTI, Robson. *Internet em benefício do acesso a informação jurídica*, página da web [http://www.cbeji.com.br/br/novidades/artigos/main.asp?id=178]. Acesso em: 15 mar. 2006.
- ZEFF, Robin; ARONSON, Brad. *Advertising on the Internet*. 2. ed. Wiley, 1999.



Glossário

Accounting rate systems • Acerto de contas entre as telefônicas para completar ligações de Internet internacionais.

Acesso em • Conexão com a rede mediante uma porta de entrada e um protocolo IP.

ActiveX • Metodologia desenvolvida pela Microsoft em meados da década de 1990, usada principalmente com o objetivo de desenvolver conteúdos interativos para a *web*. Linguagem de programação que faz *downloads* e corre programas no disco rígido do computador. A tecnologia do ActiveX é usada pelo Microsoft Internet Explorer para criar páginas da *web*, que se pareçam e se comportem mais como programas de computador do que como páginas estáticas. Com o ActiveX, os utilizadores podem perguntar ou responder por meio de botões de pressão e interagir de muitas outras formas com a página *web*.

Add-on • Termo utilizado em relação aos programas que vêm acrescentar mais recursos a um programa maior. Também pode referir-se a qualquer *hardware* ou *software* que venham acrescentar maiores recursos ao computador.

ADSL • Do inglês *Asymmetric Digital Subscriber Line*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidades maiores que as permitidas por um *modem* convencional.

Adware • Do inglês *Advertising Software*. *Software* especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos. Pode ser considerado um tipo de *spyware*, caso monitore os hábitos do usuário, por exemplo, durante a navegação na Internet para direcionar as propagandas que serão apresentadas.

Ambiente • Nome utilizado para especificar o *software* de base do gerenciador do sistema no qual se está trabalhando. É o ambiente de trabalho que define a comunicação entre o usuário e o computador.

Anel/Ring • Rede local na qual os dispositivos (nós) ficam interligados em um círculo fechado, ou anel. Nas redes em anel, as mensagens circulam em uma única direção, de nó a nó. Conforme as mensagens percorrem o anel, cada nó examina o endereço de destino associado à mensagem. Se o endereço for igual ao endereço do nó, ele aceitará a mensagem; se não, a mensagem será regerada e passada adiante, para o próximo nó do círculo. O fato de que as mensagens são regeradas permite que as redes em anel cubram distâncias maiores que as redes em estrela e as redes de barramento. Além disso, o seu projeto pode incluir meios de evitar nós defeituosos ou inoperantes. Entretanto, em razão do círculo fechado, a inclusão de novos nós é difícil.

Antivírus • Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos.

AP • Do inglês *Access Point*. Dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Aplicações Internet • Também conhecidas como aplicações TCP/IP, são os programas de aplicações que utilizam os protocolos da rede conhecidos como: FTP para transmissão de arquivos, SMTP e POP para correio eletrônico, HTTP e HTML em *browsers*, IRC para bate-papo e outros.

Applet • Tipo de “miniprograma” que executa algumas tarefas bastante específicas e depois é descarregado da memória. Essa prática é bastante utilizada na Internet. Quando você carrega páginas sofisticadas, são disparados diversos *applets* (normalmente em linguagem Java) para, por exemplo, tocar sons, emitir mensagens, animar imagens etc. Após cumprido o seu papel, o *applet* é simplesmente descartado da memória.

Arquitetura cliente/servidor • É toda arquitetura de rede onde estações (microcomputadores) executam aplicações de clientes que se utilizam de programas servidores para transferência de dados do próprio servidor ou comunicação com outras estações e suas aplicações clientes.

Arquivo • É um agrupamento de *bits* que formam uma unidade lógica que possa ser interpretada pelo processador do PC. Na verdade, os arquivos são tudo o que compõe o *software* do computador. O sistema operacional, os aplicativos e os documentos que são manipulados pela máquina compõem-se de milhares de arquivos. Cada arquivo é definido por um nome e uma extensão. A extensão é um código universal que determina o tipo de arquivo em questão. Combinado com o nome, identifica exclusivamente o arquivo dentro de um mesmo diretório.

Artefato • De forma geral, artefato é qualquer informação deixada por um invasor em um sistema comprometido. Pode ser um programa ou *script* utilizado pelo invasor em atividades maliciosas, um conjunto de ferramentas usadas pelo invasor, *logs* ou arquivos deixados em um sistema comprometido, a saída gerada pelas ferramentas do invasor etc.

ASCII • *American Standard Code for Information Interchange*. É o Código Americano Padrão para Troca de Informações. Criada nos EUA, a codificação, que serve para padronizar todo o alfabeto e símbolos gráficos usados em computadores, foi aceita posteriormente como padrão em todo o mundo. Com este código, as letras do alfabeto, números de 0 a 9, símbolos gráficos e até mesmo códigos de controle básicos para impressora ou tela recebem números que os representam. Originalmente, o ASCII foi projetado para gastar meio *byte* e os valores foram mantidos entre 0 e 127, sendo que os números de 128 a 255, que completariam o *byte* inteiro, foram reservados para exceções. Quando usados, são normalmente chamados de *ASCII Extended* (estendido) exatamente onde ficam, por exemplo, os nossos acentos. Apesar de o ASCII ser aceito no mundo todo, o *ASCII Extended* sofreu tantas variações que é muito difícil encontrar dois iguais. No Brasil há pelo menos duas versões oficiais, uma dos fabricantes de impressoras e a outra da ABNT; de modo informal sempre valeu o *extended* dos micros IBM. Antigamente, para usar um micro era preciso ter ao lado uma tabela de ASCII, para poder programar, mas hoje o ASCII é incorporado aos códigos de teclado, que fazem as devidas conversões. O problema dos acentos, porém, nunca foi solucionado de forma satisfatória, até porque a língua inglesa não os usa. Com o tempo, ASCII passou a ser também sinônimo de textos que não levam códigos de controle específicos, como negrito, itálico ou códigos de programas tipo DTP ou editores de texto sofisticados.

Assinatura digital • Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

Atacante • Pessoa responsável pela realização de um ataque. Veja também *Ataque*.

Atalho • *Shortcut*. Ícone que pode ser colocado na tela inicial do micro para facilitar o acesso a um programa ou arquivo.

Ataque • Tentativa, bem-sucedida ou não, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço.

Ativos de informação • Patrimônio composto de todas as informações, base de dados e arquivos, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos de suporte ou operação.

Ativos de TI • Patrimônio composto de todos os ativos de informação, *hardwares*, *softwares*, licenças e demais componentes de TI.

Autoridade certificadora • Entidade responsável por emitir certificados digitais, que podem ser emitidos para diversos tipos de entidades, tais como: pessoa, computador, departamento de uma instituição, instituição etc.

Backdoor • Programa que permite a um invasor retornar a um computador comprometido. Normalmente esse programa é colocado de forma a não ser notado.

Backup • Cópia exata de um programa, disco ou arquivo de dados, feita para fins de arquivamento ou para salvaguardar arquivos importantes na eventualidade de que a cópia ativa (original) seja danificada ou destruída. Por esse motivo, o *backup* também é chamado de cópia de segurança. Alguns programas aplicativos fazem automaticamente cópias de *backup* dos arquivos de dados, mantendo em disco tanto a versão atual quanto a versão anterior.

Banco de dados • Arquivo composto de registros, contendo cada um deles campos, com um conjunto de operações para pesquisa, classificação, recombinação e outras funções.

Banner • O termo *banner* remete usualmente para os estandartes, as bandeiras e as insígnias. Historicamente, tem sido aplicado para definir os cargos de poder, as marcas de negócio, as imagens políticas, os territórios tribais, e nas páginas *web* os *banners* têm um estatuto idêntico, com a novidade acrescida de funcionar como os reclamos dos néons.

BISDN • *Broadband Integrated Services Digital Network*, rede digital de serviços integrados em banda larga. Utiliza fibra óptica e permite uma taxa de transferência de 155 *megabits* por segundo.

Bluetooth • Termo que se refere a uma tecnologia de radiofrequência (RF) de baixo alcance, utilizada para a transmissão de voz e dados.

Boato • *E-mail* que possui conteúdo alarmante ou falso e, geralmente, tem como remetente — ou aponta como autora da mensagem — alguma instituição, empresa importante ou órgão governamental. Mediante uma leitura minuciosa desse tipo de *e-mail*, normalmente é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Bot • Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente por meio da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente. O invasor, ao se comunicar com o *bot*, pode orientá-lo a desferir ataques contra outros computadores, furtar dados, enviar *spam* etc.

Broadband • Banda larga, rede de alta capacidade que pode transmitir simultaneamente dados, áudio e vídeo.

Browser • Significa pesquisar, e podemos traduzi-lo como navegador. Na Internet, o termo deve ser interpretado como uma ferramenta que permite a paginação ou folheamento. O termo acabou virando um sinônimo para os programas que permitem acessar e mostrar as *home pages* encontradas na *web*. O primeiro *browser* a permitir o acesso gráfico, o MOSAIC, criado numa universidade americana, serviu de padrão para a criação do conceito de *web*. Atualmente, várias empresas estão disputando o mercado para impor seus produtos e modificar os padrões atuais. Os programas, que anteriormente serviam apenas para permitir a visualização de páginas escritas em HTML, estão evoluindo e incorporando outras atividades, tais como leitura de *e-mail*. Um *browser* é ferramenta indispensável para poder acessar a Internet graficamente, e com o surgimento de novas linguagens de criação das *home pages* os *browsers* têm se sofisticado cada vez mais, para poder suportar tais avanços.

Cable modem • *Modem* especial que utiliza a rede de televisão a cabo para transmitir e receber dados, em vez da tradicional linha telefônica, alcançando maior velocidade.

Cavalo de troia • Programa, normalmente recebido como um “presente” (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo etc.), que executa não só as funções para as quais foi aparentemente projetado, mas também outras funções normalmente maliciosas e sem o conhecimento do usuário.

Certificado digital • Identidade digital ou ID digital, permite a codificação e a assinatura de mensagens para assegurar sua autenticidade, integridade e inviolabilidade. É muito utilizado em páginas comerciais na Internet. Ou arquivo eletrônico, assinado digitalmente, que contém dados de uma pessoa ou instituição utilizados para comprovar sua identidade. Veja também *Assinatura digital*.

Chat/Internet relay chat • Conversa em tempo real pelo computador. Quando um participante digita uma linha de texto e, em seguida, pressiona a tecla *enter*, suas palavras aparecem nas telas dos outros participantes, que podem responder da mesma forma. A maioria dos serviços *online* suporta o bate-papo na Internet.

Classificação da informação • Categorização da informação quanto à confidencialidade, integridade, disponibilidade e idade documental para o negócio da organização à qual pertence.

Client • Cliente. No contexto cliente/servidor, cliente é um programa que pede determinado serviço (por exemplo, a transferência de um arquivo) a um servidor, outro programa ou computador. O cliente e o servidor podem estar em duas máquinas diferentes, sendo esta a realidade para a maior parte das aplicações que usa esse tipo de interação. É um processo ou programa que requisita serviços a um servidor.

Código malicioso • Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador. Exemplos de códigos maliciosos são os vírus, *worms*, *bots*, cavalos de troia, *rootkits* etc.

Colaborador • É todo empregado, empregado de terceiros, parceiro, estagiário ou pessoa que venha a ter acesso a informações da empresa.

Comércio eletrônico • Também chamado de *e-commerce*, é qualquer forma de transação comercial em que as partes interagem eletronicamente. Conjunto de técnicas e tecnologias computacionais utilizada para facilitar e executar transações comerciais de bens e serviços pela Internet.

Compartilhamento • Disponibilização de arquivos ou recurso fisicamente ligados a um terminal de uma rede para outros terminais. Compartilham-se *windows*, arquivos, diretórios, impressoras, *scanners* e outros periféricos.

Compatibilidade • Característica de sistemas informatizados (*hardware* e *software*) que funcionam conforme padrão comum. Podem-se determinar diferentes graus de compatibilidade. Quanto mais compatíveis, menos diferentes serão dois ou mais sistemas.

Compra coletiva • É uma modalidade de *e-commerce* que vende produtos ou prestação de serviços para um número mínimo determinado de consumidores por oferta.

Compressão de dados • É a técnica utilizada pelos *modems* para transmitir dados em taxas mais elevadas. O *modem* que recebe esses dados fará a descompressão pela mesma técnica.

Comunicação particular • Comunicação cujo conteúdo é endereçado com exclusividade a um ou mais destinatários determinados pelo remetente.

Comunicação pública • Comunicação cujo conteúdo é endereçado a destinatários não determinados individualmente pelo remetente ou fornecedor de conteúdo.

Conexão segura • Conexão que utiliza um protocolo de criptografia para a transmissão de dados, por exemplo, HTTPS ou SSH.

Confidencialidade • Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Consumidor digital • Todo aquele que consome produtos e/ou serviços disponíveis na rede Internet.

Conteúdo • Qualquer informação multimídia (em formato texto, imagem, som, programa de computador, gráficos) publicada por meio da rede aberta ou fechada (acesso restrito).

Cookies • Absorventes de textos com informações sobre o comportamento dos usuários na rede. Permitem que servidores gravem informações de seu interesse em outro microcomputador remoto. Podem ou não ser configurados no *browser*.

Coopetição • Sistema de negócios que reúne competição e colaboração entre empresas.

Correção de segurança • Correção especificamente desenvolvida para eliminar falhas de segurança em um *software* ou sistema operacional.

Cracker • Uma espécie de pirata virtual, que penetra remotamente em computadores integrados à rede com o objetivo de causar algum dano ou obter informações ilegalmente.

Criptografia • Método de codificação de dados que permite o acesso apenas de pessoas autorizadas, possuidoras de chave de acesso. Ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, entre outras finalidades, para autenticar a identidade de usuários e autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos e proteger o sigilo de comunicações pessoais e comerciais.

Criptografia assimétrica • Sistema de segurança para transmissões eletrônicas que trabalha com tecnologia de chaves assimétricas.

Cyberspace • Ciberespaço. Assim se designa habitualmente o conjunto das redes de computadores e serviços existente na Internet. É uma espécie de planeta virtual, no qual as pessoas se relacionam virtualmente, por meios eletrônicos. Termo inventado por William Gibson no seu romance *Neuromancer* e idealizado em analogia com o espaço sideral explorado pelos astronautas.

Day-trade • Operação financeira em que a tomada, a execução e a liquidação ocorrem no mesmo dia.

Device • Termo em inglês que define dispositivo, muito utilizado para se referir a tecnologias de uso individual, como celular, *palm* e computador.

Dial-up • A rede ou conexão *dial-up* é a porta de comunicação entre o computador e a Internet via linha discada. É composto de uma série de funções e protocolos (principalmente o TCP/IP) que permite ao computador entrar em rede e conversar com a *Net* por meio de um *modem*, informando um número de linha discada de um provedor pago e um endereço da *web*.

Disclaimer • Declaração aberta disponível em *website* de Internet que traz termos com responsabilidades e obrigações cuja leitura e continuação da operação pressupõem aceitação das condições declaradas.

Disclosure • Termo em inglês para definir transparência, mais comumente utilizado no mercado financeiro.

Display • Termo utilizado para definir dispositivo de tela.

Disponibilidade • Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

DNS • Domain Name Server. Na Internet, é o sistema por meio do qual *hosts* têm endereços de nome de domínio e endereços IP. O endereço de nome de domínio é utilizado pelos usuários e automaticamente traduzido no endereço IP, que é utilizado pelo *software* de roteamento de pacotes.

Domain name ou Domínio • Nome que descreve a organização com a qual um endereço na Internet está vinculado. Faz parte da hierarquia de nomes de grupos ou *hosts* da Internet, identificando as instituições na rede. Exemplo: <http://www.embratur.gov.br>, em que *embratur* indica a localização do servidor.

DoS • Denial of Service, ataque *hacker* que consiste em fazer com que o seu computador ou um servidor *web* pare de responder ou até mesmo trave por um excesso de processos solicitados, o que resulta numa negação de serviço.

Download • Ato de transferir o arquivo de um computador remoto para o seu próprio computador, usando qualquer protocolo de comunicações. Processo de transferência de cópia de um arquivo em um computador remoto para outro computador pela rede. O arquivo recebido é gravado em disco no computador local. Ver também *FTP*.

Dynamic HTML • É um termo abrangente para uma combinação das novas etiquetas e opções, *style sheets* e programação de *HyperText Markup Language* (HTML), que permitem criar páginas *web* mais animadas e com mais interatividade com o utilizador do que as versões anteriores de HTML. Há mais especificações do *Dynamic HTML* no HTML 4.0. O *Dynamic HTML* permite que os documentos da *web* funcionem como aplicações de computador ou produções multimídia e pareçam com essas aplicações.

E-book • Livro em formato eletrônico que pode ser baixado pela Internet.

E-business • Palavra que identifica transações e comércios pela Internet que estão baseados em algum sistema de *e-commerce*. Qualquer tipo de negócio efetuado por meio da rede mundial é tratado como um *e-business*.

E-commerce • Comércio eletrônico baseado na atividade de compra e venda de bens e/ou serviços feita totalmente ou em parte por meio da rede Internet.

Electronic Data Exchange • Troca eletrônica de dados mediante sistemas aplicativos previamente programados.

E-mail bombing • É o envio de *e-mails* imensos ou vários *e-mails*, que causa atraso na recepção.

E-mail com vírus • É o envio de vírus anexado ao *e-mail*.

Endereço IP • É o endereço real de uma máquina na Internet. Consiste em uma série de números separados por pontos. Cada máquina conectada à rede tem um endereço IP. Os *Domain Name Servers* servem então para relacionar os "endereços com letras" com o endereço IP.

Engenharia social • Método de ataque em que uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores.

Ethernet • Arquitetura de redes local, baseada na norma IEEE 802.3, que define o método de disputa para redes. Utiliza uma topologia em estrela ou de barramento e baseia-se na forma de acesso conhecida como CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*) para controlar o tráfego nas linhas de comunicação. Os nós da rede são ligados por cabos coaxiais, por cabos de fibra óptica ou por fios de pares trançados.

Exploit • Programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um *software* de computador.

Fair use • Termo que define "uso justo" em matéria de direito autoral.

Falsa identidade • Ato em que o falsificador se atribui identidade ilegítima, podendo se passar por outra pessoa, com o objetivo de conseguir vantagens indevidas, por exemplo, obter crédito, furtar dinheiro de contas bancárias das vítimas, utilizar cartões de crédito de terceiros, entre outras.

FAQ • Frequently Asked Questions. É um texto que pretende responder, dentro de uma determinada matéria, a questões colocadas frequentemente pelos usuários. É o documento com perguntas e respostas, em geral voltado para leigos.

Firewall • Uma *firewall* consiste em um *hardware* e/ou *software* que se interpõe entre duas redes, por exemplo, uma rede interna e um fornecedor de serviço Internet. A *firewall* protege sua rede impedindo o acesso de utilizadores indesejáveis e a passagem de mensagens para receptores específicos externos à rede, tais como os concorrentes.

Fornecedor de acesso • Todo aquele que fornece o serviço de acesso à Internet.

Fornecedor de conteúdo • Todo aquele que produz, emite, edita e/ou publica conteúdo na Internet.

Fornecedor de hosting • Todo aquele que fornece o serviço de *hosting* ou servidor conectado à Internet.

Forum/News Group • Espaço virtual de debate com caráter temático, comunicação deferida e constituída por mensagens propagadas por meio da rede em todos os servidores que hospedam o debate eletronicamente.

Frame • *Frames* são subdivisões da janela principal do navegador (ou *browser*). Cada subdivisão funciona como uma pequena janela, exibindo conteúdos independentes. Os criadores de *sites* da *web* utilizam esse recurso quando é necessário exibir muitas informações de uma só vez. Normalmente eles montam um *frame* à esquerda da página, o qual funciona como um índice, enquanto o *frame* da direita exibe o conteúdo relacionado ao *link* do índice que o usuário selecionou.

Freeware • Programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso. Em geral, o *software* é utilizável sem custos para fins estritamente educacionais, e não tem garantia de manutenção ou atualização. Um dos grandes trunfos da Internet é a quantidade praticamente inesgotável de domínio público, com excelente qualidade, que circula pela rede.

FTP • *File Transfer Protocol*. Designa o principal protocolo de transferência de arquivos usado na Internet, ou então um programa que usa esse protocolo. Um protocolo-padrão da Internet que é usado para transferência de arquivos entre computadores.

Gerenciador de Banco de Dados • Interface de *software* entre o banco de dados e o usuário. Um sistema de gerenciamento de bancos de dados que trata de solicitações do usuário para ações de bancos de dados e permite o controle centralizado da segurança e da integridade dos dados.

Gerenciamento de risco • Processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável.

GnuPG • Conjunto de programas gratuito e de código aberto, que implementa criptografia de chave única, de chaves pública e privada e assinatura digital.

GPG • Veja *GnuPG*.

GPS • *Global Positioning System*. Consiste numa “constelação” de 24 satélites que estão na órbita da Terra a uma altura de 10.900 milhas, tornando possível às pessoas que utilizem receptores no solo determinar sua posição geográfica entre 10 e 100 metros.

Hackers • Indivíduo que faz todo o possível e o impossível para entrar num sistema de informática alheio, quebrando sistemas de segurança, para assim poder causar danos.

Harvesting • Técnica utilizada por *spammers* que consiste em varrer páginas *web*, arquivos de listas de discussão, entre outros, em busca de endereços de *e-mail*.

HDTV • *High Definition Television*. Termo em inglês que define a tecnologia de televisão de alta definição.

Hipermídia • Documento que contém imagens, sons, textos e vídeos, utilizando ligações de hipertextos para permitir o acesso a outro documento.

Hipertexto • São palavras marcadas no texto que permitem acesso a outros documentos relacionados com o assunto em questão, criando uma linha de pesquisa. Normalmente estão sublinhadas.

Hipertextos • Formato das informações dispostas na Internet.

Hoax • Veja *Boato*.

Home broker • Corretora de valores que pode ser acessada de casa por telefone ou pela Internet e que efetua operações remotas. O termo começou a ser usado para definir os serviços de corretagem, assim como se usa o termo *home banking* para o serviço de acesso ao banco em casa por sistema de discagem ou eletrônico.

Homepage • Assim é chamada a página de abertura de um serviço ou de uma página pessoal. Da *homepage* você pode acessar outras páginas por meio dos *hyperlinks*.

Host • Computador principal de um sistema de computadores ou terminais conectados por enlaces de comunicação.

Hosting • Hospedagem eletrônica locando parte do servidor para distribuição de conteúdos e serviços pela rede.

HTM (HTML) • Extensão para arquivos gerados e salvos no formato *HiperText Marked Language* (Linguagem de Hipertexto Marcado), para construção de *homepages*. As versões oficiais da HTML são definidas pelo *W3 Consortium*, em <http://w3.org>.

HTTP • *HyperText Transfer Protocol*. Este é o protocolo usado para transportar tráfego entre o computador do *browser* da *web* e o *site* da *web*.

HTTPS • Quando utilizado como parte de uma URL, especifica a utilização de HTTP com algum mecanismo de segurança, normalmente o SSL.

Identidade virtual • Identidade de usuário que entra na rede de computadores Internet formada pela junção de códigos IP — e-mail — RG ou CPF.

IDS • Do inglês *Intrusion Detection System*. Programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

IEEE • Acrônimo para *Institute of Electrical and Electronics Engineers*, organização composta por engenheiros, cientistas e estudantes que desenvolvem padrões para a indústria de computadores e eletroeletrônicos.

Incidente de segurança • É qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo tratado pela política de segurança.

Incubadoras • Empresas que têm como finalidade alavancar ideias e transformá-las em negócios.

Informação • É um ativo composto por um conjunto de dados ou elementos que, como qualquer outro ativo importante para os negócios, tem valor para a organização e, conseqüentemente, necessita ser adequadamente protegido.

Infraestrutura • Linhas e aparelhos de telecomunicação necessários ao funcionamento da rede.

Integridade • Garantia de salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Internet • Rede mundial de computadores e outros dispositivos interligados que possibilitam acesso à informação nela disponibilizada.

Intranet • São redes corporativas que se utilizam da tecnologia e infraestrutura de comunicação de dados da Internet. São utilizadas na comunicação interna da própria empresa e/ou na comunicação com outras empresas.

Invasão • Ataque bem-sucedido que resulte em acesso, manipulação ou destruição de informações em um computador.

Invasor • Pessoa responsável pela realização de uma invasão (comprometimento). Veja também *Invasão*.

IP • *Internet Protocol*, protocolo responsável pelo percurso de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na Internet.

ISP • *Internet Service Provider*. Uma empresa que vende ligações à *Net*.

Keylogger • Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do *keylogger* é condicionada a uma ação prévia do usuário, por exemplo, após o acesso a um *site* de comércio eletrônico ou *Internet Banking*, para a captura de senhas bancárias ou números de cartões de crédito.

Largura de banda • Quantidade de dados que podem ser transmitidos em um canal de comunicação, em determinado intervalo de tempo.

Link • Elo ou ligação. Conexão entre um elemento de um documento de hipertexto, como uma palavra, expressão, símbolo ou imagem, e outro elemento do documento, outro documento de hipertexto, um arquivo ou um *script*. O usuário ativa o vínculo dando um clique sobre o elemento vinculado, que é geralmente sublinhado ou apresentado em cor diferente do restante do documento para indicar que o elemento está vinculado. Os *links* são indicados em um documento de hipertexto por meio de *tags* de linguagens de marcação, como a SGML e a HTML. Em geral, essas *tags* não são visíveis ao usuário.

Log • Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls* ou por IDSs.

Lojas virtuais • São páginas que oferecem um canal direto de compra na forma de catálogos eletrônicos. O consumidor encomenda mercadorias por meio de formulários eletrônicos.

Mail box • Caixa postal eletrônica.

Mailling list • Uma lista de assinantes que se correspondem por correio eletrônico. Quando um dos assinantes escreve uma carta para determinado endereço eletrônico (de gestão da lista), todos os outros a recebem, o que permite que se constituam grupos (privados) de discussão pelo correio eletrônico.

Malware • Do inglês *Malicious software* (*software* malicioso). Veja *Código malicioso*.

M-commerce • É o *e-commerce* realizado em plataforma móvel como telefones celulares, PDAs etc.

MMS • Do inglês *Multimedia Message Service*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de dados, como texto, imagem, áudio e vídeo.

Modem • Modulador DEModulador. Conversor de sinais analógicos (linha telefônica) em sinais digitais (microcomputador) e vice-versa. É usado para ligações entre computadores por meio da linha telefônica. Ao adicionar-se uma placa FAX/MODEM, ampliam-se os recursos de microcomputador.

MP3 • MP3, que significa *Motion Picture Experts Group-Layer 3*, é um formato de compressão de áudio que cria ficheiros com uma qualidade próxima dos CDs, os quais são 10 ou 20 vezes menores que os ficheiros de música ou os CDs normais. O MP3 torna possível mover ficheiros de som de alta qualidade através de um *modem* e pode armazenar 150 canções num CD.

Napster • Tecnologia de compartilhamento de arquivos na Internet que possibilita acesso e compartilhamento de música.

Negação de serviço • Atividade maliciosa em que o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à Internet.

Opt-in • Regra de envio de mensagens que define ser proibido mandar *e-mails* comerciais/*spam*, a menos que exista uma concordância prévia por parte do destinatário. Veja também *Soft opt-in*.

Opt-out • Regra de envio de mensagens que define ser permitido mandar *e-mails* comerciais/*spam*, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

P2P • Acrônimo para *peer-to-peer*. Arquitetura de rede em que cada computador tem funcionalidades e responsabilidades equivalentes. Difere da arquitetura cliente/servidor, em que alguns dispositivos são dedicados a servir outros. Esse tipo de rede é normalmente implementada via *softwares* P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens etc.

Page-views • Termo que define "páginas vistas" e é usado como sistema de métrica e medição de resultado de comunicação na Internet.

Password • Veja *Senha*.

Patch • Veja *Correção de segurança*.

Pay-per-download • Serviço de acesso a conteúdo em que se paga no ato de baixar o arquivo por *download*.

Pay-per-play • Serviço de acesso a conteúdo em que se paga no ato de jogar o conteúdo.

Pay-per-use • Serviço de acesso a conteúdo em que se paga para usar o conteúdo.

Pay-per-view • Serviço de acesso a conteúdo em que se paga no ato de ver o conteúdo.

PDV • Termo que define Ponto de Venda.

Peering points — Locações em que o tráfego nacional e regional da Internet podem ser trocados.

PGP • Do inglês *Pretty Good Privacy*. Programa que implementa criptografia de chave única, de chaves pública e privada e assinatura digital. Possui versões comerciais e gratuitas.

Phishing • Também conhecido como *phishing*. Mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. Atualmente, o termo também se refere à mensagem que induz o usuário à instalação de códigos maliciosos, além da mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros.

Piratas de computador • Definição usada para referir-se aos *hackers*.

Players • Termo usado para definir as partes envolvidas em uma operação ou mercado específico.

Ponto de presença • 1. Ponto de uma rede remota ao qual um usuário pode conectar-se mediante uma chamada telefônica local. 2. Ponto em que uma concessionária telefônica de longa distância se conecta a uma central telefônica local ou a um usuário específico.

Pop-up • Formato de comunicação usado na Internet que tem como principal característica aparecer na tela sem ter sido solicitado, por isso, o termo *pop-up*.

Portais horizontais • Portais que têm uma estratégia de oferta de conteúdo e serviços horizontais, ou seja, em que um não está diretamente relacionado ao outro. É multidisciplinar.

Portais verticais • Portais que têm uma estratégia de oferta de conteúdo e serviços verticais, ou seja, em que um é complementar ao outro dentro de uma cadeia específica de negócio.

PPP • *Point to Point Protocol*. O PPP implementa o protocolo TCP/IP numa linha telefônica, sendo por meio desta que um computador pessoal se liga à Internet e pode usufruir de todos os serviços e aplicações existentes. É posterior ao SLIP e mais completo.

Protocolo • Código que permite a leitura universal da informação.

Provedor de Acesso • Instituição que se liga à Internet, via um ponto de presença ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos e instituições, em caráter comercial ou não. O provedor de acesso torna possível ao usuário final a conexão à Internet por meio de uma ligação telefônica local.

Proxy • Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet. *Proxies* mal configurados podem sofrer abusos por atacantes e serem utilizados como forma de tornar anônimas algumas ações na Internet, como atacar outras redes ou enviar *spam*.

Realidade virtual • É qualquer uma das várias combinações de recursos de interface de usuário que permite a ele interagir com o computador ou sistema, de maneira tal que tenta imitar da forma mais perfeita possível o ser humano. Pode incluir vários tipos de recursos.

Rede sem fio • Rede que permite a conexão entre computadores e outros dispositivos por meio da transmissão e recepção de sinais de rádio.

Redes sociais • São plataformas *online* que reúnem pessoas em torno de um mesmo interesse. Exemplos: *Facebook*, *Twitter*, *LinkedIn*, *Orkut* etc. (Fonte: <<http://imasters.com.br/artigo/21183redes-sociais/o-que-sao-redes-sociais-corporativas-e-quais-sao-suas-vantagens>>. Acesso em: 1º-1-2011 às 17:37).

Rootkit • Conjunto de programas que tem como finalidade esconder e assegurar a presença de um invasor em um computador comprometido. É importante ressaltar que o nome *rootkit* não indica que as ferramentas que o compõem são usadas para obter acesso privilegiado (*root* ou *administrator*) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido.

Roteador • *Router*. Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Uma instituição, ao se conectar à Internet, deverá adquirir um roteador para conectar sua rede local ao ponto de presença mais próximo. Roteadores vivem se falando aos pares, como *modems*.

Scam • Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan • Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja *Scanner*.

Scanner • Programa utilizado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador. Ou dispositivo óptico de entrada que usa sensores de luz para capturar uma imagem no papel ou algum outro meio. A imagem é traduzida em sinais digitais que podem ser processados por *softwares* de reconhecimento de caracteres ópticos (OCR) ou *softwares* gráficos. Há diversos tipos de *scanners*, entre eles: de mão (o usuário passa o dispositivo sobre um documento estático), de mesa (o cabeçote de varredura é movimentado sobre um documento fixo), com alimentação de papel (o documento é passado sobre um cabeçote de varredura estático), tambor (o documento é girado ao redor de um cabeçote de varredura estática).

Screenlogger • Forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou armazenar a região que circunda a posição em que o *mouse* é clicado. Veja também *Keylogger*.

Segurança da informação • Protege a informação de uma gama extensiva de ameaças para assegurar a continuidade dos negócios, minimizar os danos empresariais e maximizar o retorno em investimentos e oportunidades. É caracterizada pela preservação da confidencialidade, integridade e disponibilidade.

Senha • Conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser.

Server • Servidor. É o computador que administra e fornece programas e informações para os outros computadores conectados. No modelo cliente-servidor, é o programa responsável pelo atendimento a determinado serviço solicitado por um cliente. Serviços como *archie*, *gopher*, *WAIS* e *web* são providos por servidores. Referindo-se a equipamento, o servidor é um sistema que provê recursos tais como armazenamento de dados, impressão e acesso *dial-up* para usuários de uma rede de computadores.

Shareware • *Software* que é distribuído livremente, desde que seja mantido o seu formato original, sem modificações, e seja dado o devido crédito a seu autor. Normalmente é feito para ser testado durante um curto período de tempo. Terminado

o período, o usuário tem a opção de enviar o pagamento a seu autor para ser registrado. Por ocasião do registro, recebe-se um manual impresso do programa, assim como uma versão melhorada. Há ainda a possibilidade de assistência técnica e informações acerca de novas versões.

Sistema de Pagamento Seguro (SPS) • Sistema de pagamento eletrônico que possui *software* de segurança e *firewall*, utilizado, principalmente, em Bancos.

Sistema de proteção • Módulo do sistema operacional que controla o acesso aos recursos por parte de programas e usuários, possibilitando a criação de controles, dá suporte à sua execução, autentica operação e mantém registro de operações feitas para auditoria e análises de performance.

Site • Local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações multimídia.

SMS • Do inglês, *Short Message Service*. Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferentemente do MMS, permite apenas dados do tipo texto e cada mensagem é limitada em 160 caracteres alfanuméricos.

SMTP • *Simple Mail Transfer Protocol*. Protocolo Internet usado para correio eletrônico.

Sniffer • Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), nos casos em que estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Sockets • O nome da interface que implementa os protocolos TCP/IP. Interface é um conjunto de chamadas possíveis a bibliotecas que contém rotinas que implementam determinados objetivos.

Soft opt-in • Regra semelhante ao *opt-in*, mas esse caso prevê uma exceção quando já existe uma relação comercial entre remetente e destinatário. Dessa forma, não é necessária a permissão explícita por parte do destinatário para receber *e-mails* do remetente. Veja *Opt-in*.

Software • Programas de computador; instruções que o computador é capaz de entender e executar.

Spam • Termo usado para se referir a *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem também é referenciada como UCE (do inglês, *Unsolicited Commercial E-mail*).

Spammer • Pessoa que envia *spam*.

Spyware • Termo utilizado para se referir a uma grande categoria de *software* que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser utilizado de forma legítima, mas, na maioria das vezes, é usado de forma dissimulada, não autorizada e maliciosa.

SSH • Do inglês, *Secure Shell*. Protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferência de arquivos etc.

SSID • Do inglês, *Service Set Identifier*. Conjunto único de caracteres que identifica uma rede sem fio. O SSID diferencia uma rede sem fio de outra, e um cliente normalmente só pode conectar em uma rede sem fio se puder fornecer o SSID correto.

SSL • Sistema de Validação de Cartões Online. O *Secure Sockets Layer* (SSL) é um protocolo que protege os dados enviados entre *web browsers* e servidores *web*. SSL também garante que os dados vieram do *website* de que é suposto terem vindo e que ninguém interferiu com os dados enquanto estavam a ser enviados. Qualquer morada de um *website* que começa com “https” está habilitada para SSL. Fornece confidencialidade e integridade na comunicação entre um cliente e um servidor, por meio do uso de criptografia.

Sujeitos da Internet • Toda pessoa física ou jurídica conectada à rede direta ou indiretamente.

T-banking • É a oferta de serviços de Bancos por meio da televisão interativa.

T-commerce • É o comércio eletrônico por meio da televisão interativa.

TCP/IP — Protocolo para a comunicação entre computadores. O TCP/IP tornou-se o padrão de fato para transmissão de dados por meio de redes, incluindo a Internet.

TCP • *Transmission Control Protocol*. O protocolo dentro do TCP/IP que controla a subdivisão das mensagens de dados em pacotes a serem enviados por meio do protocolo IP e a remontagem e verificação das mensagens completas dos pacotes recebidos pelo IP.

Tecnologia Streaming • Tecnologia *streaming*, também conhecida por *streaming media*, permite ao utilizador ver e ouvir conteúdos digitalizados — vídeo, som e animação — apenas fazendo um *download*. As imagens e os sons *streamed* estão normalmente disponíveis por meio de um simples *plug-in* e a distância de um clique. Mas o preço dessa conveniência é a qualidade. As tecnologias de compressão usadas para transportar os conteúdos que exigem imensa amplitude de banda na Internet podem produzir imagens menos que satisfatórias, particularmente a velocidades de transmissão de 28,8 Kbps.

Time zone • Fuso horário.

TLDs • *Top Level Domain* (com, gov, net, org, tv).

Trojan horse • Veja *Cavalo de troia*.

UCE • Do inglês, *Unsolicited Commercial E-mail*. Termo usado para se referir aos *e-mails* comerciais não solicitados.

UIT • União Internacional de Telecomunicações.

Upgrade • O mesmo que atualização. Passar para uma versão mais nova, geralmente mais poderosa ou mais sofisticada de um programa.

Upload • Em português, carregar. Operação de transferência de um arquivo ou de uma página da Internet do computador para um provedor de acesso.

URL • *Universal Resource Location*. É um identificador na Internet que mostra qual tipo de servidor deve ser acessado, o equipamento em que a informação reside e sua localização nesse equipamento, por exemplo: <http://www.patriciapeck.com.br>.

Usuário • Todo aquele que acessa a rede Internet.

Venture capital • O *venture capital* (capital de risco) já foi uma área dominada por empresários de grande estatuto. Hoje, porém, as empresas entraram no negócio de maneira muito forte. Os empresários voltam-se para as empresas de capital de risco com o objetivo de conseguir fundos monetários para aplicar a ideias de negócio pensadas numa lógica de rentabilidade e já analisadas à luz do mercado para ver se eventualmente funcionarão.

Vírus • Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa tornar-se ativo e dar continuidade ao processo de infecção.

Voice-IP • Tecnologia utilizada para transmitir voz por meio de uma rede IP, ou seja, por meio de *Internet Protocol*.

VPN • Do inglês *Virtual Private Network*. Termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

VRML • *Virtual Reality Markup Language*. Formato padrão para representar a 3ª dimensão — seria o 3D, em vetor gráfico. Foi superado pelo X3D.

Vulnerabilidade • Falha no projeto, na implementação ou na configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

WAP • *Wireless Application Protocol*. É um conjunto de especificações, desenvolvida pelo WAP Forum, que permite aos programadores usar a linguagem *Wireless Markup Language* (WML) para montar aplicações em rede destinadas a dispositivos de mão sem fios. O WAP foi concebido para funcionar dentro dos limites de tais dispositivos: uma memória e potência de *Central Processing Unit* (CPU) limitadas; visores pequenos e monocromáticos; baixa largura de banda; e conexões algo instáveis.

Web bug • Imagem, normalmente muito pequena e invisível, que faz parte de uma página *web* ou de uma mensagem de *e-mail*, e que é projetada para monitorar quem está acessando essa página *web* ou mensagem de *e-mail*.

WEP • Do inglês, *Wired Equivalent Privacy*. Protocolo de segurança para redes sem fio que implementa criptografia para a transmissão dos dados. Esse protocolo apresenta algumas falhas de segurança.

Wi-Fi • Do inglês, *Wireless Fidelity*. Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

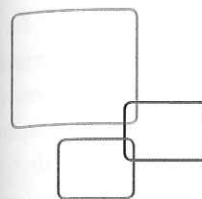
Wireless • Do inglês, “sem fio”.

WLAN • Do inglês *Wireless Local-Area Network*. Refere-se a um tipo de rede que utiliza ondas de rádio de alta frequência, em vez de cabos, para a comunicação entre os computadores.

Worm • Programa capaz de se propagar automaticamente por meio de redes, enviando cópias de si mesmo de computador para computador. Diferentemente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá mediante a exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

WPA • Do inglês, *Wi-Fi Protected Access*. Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP, devido a suas falhas de segurança. Essa tecnologia foi projetada para, por meio de atualizações de *software*, operar com produtos *Wi-Fi* que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.

WWW • Sistema de acesso e utilização de informações da Internet por meio de hipertextos com capacidade de ler e transmitir várias tecnologias e tipos de documentos, identificados todos os conteúdos por um só endereço URL.



FAQ — Perguntas e respostas sobre Direito Digital

O que é Direito Digital?

Direito Digital é o conjunto de regras e códigos de conduta que rege o comportamento e as novas relações dos indivíduos cujo meio de ocorrência ou prova da manifestação de vontade seja o digital, gerando dados eletrônicos que consubstanciam e representam as obrigações assumidas e sua respectiva autoria. Deve, portanto, reunir princípios, leis e normas de autorregulamentação que atendam ao novo cenário de interação social não presencial, interativo e em tempo real. O Direito Digital é, portanto, a evolução do próprio direito, para atender às mudanças de comportamento e às necessidades de novos controles de conduta gerados pelo uso da Tecnologia.

Há leis no Direito Digital?

As leis do Direito Digital são as mesmas já existentes, totalmente válidas e aplicáveis: a Constituição Federal de 1988, o Código Civil, o Código de Defesa do Consumidor, o Código Penal etc. Há uma série de novas leis e projetos de lei que visam a atender a questões novas específicas do uso da tecnologia, referentes a pirataria de *software*, comércio eletrônico, direitos autorais, crimes eletrônicos, além de Regulamentações e Tratados Internacionais. Tudo isso compõe o quadro normativo do Direito Digital atual.

O que fazer para reduzir os riscos da tecnologia no negócio?

O primeiro passo é realizar uma auditoria legal de risco, de modo a identificar as vulnerabilidades e, então, elaborar um plano corretivo e preventivo. Essa análise deve abordar três interfaces estratégicas de usuários da empresa que são: 1) Funcionários e Colaboradores; 2) Clientes; e 3) Parceiros e Fornecedores.

O que fazer se a minha empresa sofrer uma denúncia de Spam?

O primeiro passo é analisar a origem da denúncia e verificar se a empresa foi colocada em alguma *Black List* Internacional, o que poderá prejudicar os envios de *e-mail* da operação. Depois, é importante envolver a área de comunicação e a diretoria para decidir se será feito algum esclarecimento formal ao público da empresa e revisar os processos atuais de disparo de *e-mail marketing* e *newsletters* para identificar se não há práticas atuais que ferem a ética *online* e as boas práticas de Direito Digital.

O que fazer se a minha empresa sofrer uma denúncia de Scam?

O primeiro passo é mobilizar a área de TI ou de Segurança da Informação para rastrear a origem do *Scam*. É importante de imediato já colocar um aviso no *site* da empresa e um texto no FAQ, no tire-dúvidas do *Call Center* e no Fale Conosco, esclarecendo e avisando aos usuários e clientes que o *e-mail* falso que está circulando não é da empresa. A agilidade é crucial para minimizar as contingências neste cenário.

Sou responsável pelo mau uso da tecnologia por meus funcionários?

Em princípio, sim, a empresa é responsável solidariamente pelo mau uso das ferramentas de trabalho por seus empregados, sejam elas tecnológicas ou não, dentro da modalidade de *culpa in vigilando*.

O que é necessário para poder fazer monitoramento na empresa?

É necessário ter uma Política Digital de uso de *e-mail* e tecnologia pelos funcionários e colaboradores, que deve ser redigida de modo adequado, objetivo, proporcional, com regras claras sobre o que é certo e errado no uso da ferramenta dentro da empresa, separando o que é corporativo do que é pessoal. Essa política deve ser assinada por todos, por meio de um Termo de Ciência, ou anexada ao contrato de trabalho, sendo recomendável também a execução de um treinamento específico para instrução das novas regras. Se a empresa compartilhar dados e acessos com terceiros, que sejam colaboradores, *free lancers*, fornecedores frequentes, recomendamos a criação de uma política que preveja esses casos também.

O que é prova digital?

É o conjunto de evidências e arquivos eletrônicos que representam a relação e/ou obrigação gerada, acordada ou contratada por uma via digital. O mais importante é que, nessa hipótese, o arquivo original é o digital, sendo qualquer versão impressa cópia, uma vez que não permite perícia.

Por quanto tempo tenho de guardar os e-mails da empresa?

No mínimo pelo prazo legal da relação originária que ele representa (se é comercial, contratual, consumidor final, trabalhista, financeiro etc.). Recomendamos um mínimo de 1 ano (consumidor), 3 anos (civil), 5 a 7 anos (fiscal), 10

anos (penal), podendo chegar a 20 anos (alguns casos de trabalhista — RH e direito autoral), mas, dependendo do perfil de negócios da empresa, isso pode variar, para que se possa ter acessibilidade da prova jurídica necessária para a defesa da questão.

Existe seguro para riscos eletrônicos?

Sim, existe. É possível de ser contratado já na Europa, em especial na Inglaterra, na categoria de Seguro direto ou resseguro. Também já existe no Brasil, com o nome de ESURANCE, por meio do ISC, do IRB e da corretora MAPFRE.

Sou responsável pelo uso dos dados compartilhados com parceiros?

Sim, por isso a importância de deixar claro por contrato quais são os limites de uso dos dados compartilhados, qual a finalidade e principalmente o prazo de duração da cessão, para que não seja um cheque em branco sem data para expirar.

O que é informação?

Segundo o Aurélio (1995), informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza.

O que é gerenciamento do ciclo de vida da informação?

É o gerenciamento da informação ao longo de todo o seu processo de geração e armazenagem, desde a sua captação, transmissão, manipulação, gravação, conservação, comunicação, compartilhamento, até seu uso para fins de prova legal.

Como proteger a propriedade intelectual do site?

Há várias formas de protegê-la. Nenhuma evitará que haja mau uso ou infração a direito autoral, mas essas opções poderão contribuir em caso de discussão judicial ou de se vir a pleitear algum tipo de indenização. Entre elas está o registro na Biblioteca Nacional (www.bn.br), que tem categoria específica para registro de *website* como obra, ou no Cartório de Títulos e Documentos.

Como proteger a propriedade intelectual de softwares?

Os *softwares* gozam do mesmo regime de proteção das demais obras intelectuais e a sua proteção prescinde de qualquer formalidade; contudo, pela própria natureza da obra, recomendamos fortemente o seu registro junto ao INPI (www.inpi.gov.br), órgão nacional responsável pelo registro de *softwares*.

O que é um contrato de Outsourcing?

É um contrato de terceirização muito utilizado na área de TI e que possui cláusulas e características específicas, podendo assumir formatos internacionais, como o de "SLA" (*Service Level Agreement*) e "BPO" (*Business Process Outsourcing*).

Quem é o proprietário do desenvolvimento feito por terceirizado?

Depende da forma como for contratado o desenvolvimento de *software*, sendo importante distinguir o que é direito moral de autor do que são os direitos de exploração patrimonial. Para fins de registro no INPI é fundamental ter o contrato de terceirização e o contrato do funcionário/desenvolvedor.

Que fazer se alguém usar meus conteúdos e/ou marcas na Rede?

A primeira medida é a notificação, que pode ser feita pela própria via eletrônica. Se possível, verifique a origem do infrator para que seja feita uma notificação extrajudicial com pedido para que cesse o uso indevido de referido conteúdo. Pode ser ainda impetrada medida para tirar do ar a página em que o conteúdo estiver inserido. Em qualquer das hipóteses, como prevenção, é sempre importante realizar os registros adequados nos Órgãos, além de destacar a frase "Direitos Autorais Reservados", seja no rodapé do *site*, seja no interior do conteúdo de uma palestra, ou ao clicar com o botão direito do *mouse* na imagem no campo propriedades.

O que é segurança da informação?

Segundo a norma ISO/IEC 17799:2000, segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos. Ainda segundo a ISO/IEC 17799:2000, a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade.

O que é BS 7799?

O British Standard 7799 é uma norma de segurança da informação destinada a empresas. Criada na Inglaterra, teve seu desenvolvimento iniciado em 1995, dividindo-se em duas partes: A BS 7799-1 e a BS 7799-2. A BS 7799-1 é a primeira parte da norma, que contém introdução, definição de extensão e condições principais de uso da norma. Disponibiliza 148 controles divididos em dez partes distintas. É planejada como um documento de referência para implementar "boas práticas" de segurança na empresa. A BS 7799-2 é a segunda parte da norma e tem por objetivo proporcionar uma base para gerenciar a segurança da informação dos sistemas das empresas.

O que é ISO/IEC 17799?

A ISO/IEC 17799 é a versão internacional da BS 7799, homologada pela *International Standardization Organization* (ISO) em dezembro de 2000. A NBR ISO/IEC 17799 é a versão brasileira da norma ISO, homologada pela ABNT em setembro de 2001. ISO é uma organização internacional formada por um conselho e comitês com membros oriundos de vários países. Seu objetivo é criar

normas e padrões universalmente aceitos sobre como realizar as mais diversas atividades comerciais, industriais, científicas e tecnológicas. IEC significa *International Engineering Consortium*. É uma organização voltada para o aprimoramento da indústria da informação. Uma associação entre as duas instituições produz normas e padronizações internacionais.

Por que as empresas passaram a se preocupar com Segurança da Informação?

Porque na sociedade digital tudo são dados. A identidade do indivíduo, as informações de clientes, a declaração de imposto de renda, até o perfil de consumo. Logo, o negócio da empresa se passa por proteger essas informações, que exigem privacidade, sigilo, confidencialidade. Está tudo conectado e em tempo real, e a conduta de uma única pessoa, um simples *e-mail* com vírus, pode colocar a perder todo o patrimônio de uma empresa, todos os bancos de dados. Como a Internet e as ferramentas tecnológicas são novas, não está claro para as pessoas de modo geral o que é certo e errado. Já que na empresa isso é ferramenta de trabalho, cabe a ela definir com Políticas e com Segurança da Informação o que é mais adequado para a proteção do negócio e dos empregados, evitando correr riscos desnecessários que possam gerar responsabilidade civil, criminal e até demissão.

O que é um incidente de segurança?

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. São exemplos de incidentes de segurança: tentativas de ganhar acesso não autorizado a sistemas ou dados; ataques de negação de serviço; uso ou acesso não autorizado a um sistema; modificações em um sistema, sem o conhecimento, as instruções ou o consentimento prévio do dono do sistema; desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

O que pode ser considerado uso abusivo da rede?

Não há uma definição exata do que possa ser considerado um uso abusivo da rede. Internamente às empresas e instituições, situações que caracterizam o uso abusivo da rede estão definidas na política de uso aceitável. Na Internet como um todo, os comportamentos listados a seguir são geralmente considerados como uso abusivo: envio de *spam*; envio de "correntes" da felicidade e de "correntes" para ganhar dinheiro rápido; cópia e distribuição não autorizada de material protegido por direitos autorais; utilização da Internet para fazer difamação, calúnia, ameaças e fraudes; tentativas de ataques a outros computadores; comprometimento de computadores ou redes.

Por que devo notificar incidentes?

Quando um ataque é lançado contra uma máquina, ele normalmente tem uma destas duas origens: um programa malicioso que está fazendo um ataque de

modo automático, como, por exemplo, um *worm* ou um *bot*; uma pessoa que pode estar ou não utilizando ferramentas que automatizam ataques. Quando o ataque parte de uma máquina que foi vítima de um *worm* ou de um *bot*, reportar este incidente para os responsáveis pela máquina que originou o ataque vai ajudá-los a identificar o problema e resolvê-lo. Se este não for o caso, a pessoa que está atacando o seu computador pode estar violando a política de uso aceitável da rede que utiliza ou, pior ainda, pode ter invadido uma máquina e a estar utilizando para atacar outros computadores. Nesse caso, avisar os responsáveis pela máquina de onde parte o ataque pode alertá-los para o mau comportamento de um usuário ou para uma invasão que ainda não havia sido detectada.

Para quem devo notificar os incidentes?

Os incidentes ocorridos devem ser notificados aos responsáveis pela máquina que originou a atividade e também aos grupos de resposta a incidentes e abusos das redes envolvidas. De modo geral, a lista de pessoas/entidades a serem notificadas inclui: os responsáveis pela rede que originou o incidente, incluindo o grupo de segurança e abusos, se existir um para aquela rede; o grupo de segurança e abusos da rede em que você está conectado (seja um provedor, empresa, universidade ou outro tipo de instituição). Caso algum dos *sites* envolvidos seja brasileiro, mantenha o CERT.br (cert@cert.br) na cópia da mensagem.

Por que devo manter o CERT.br na cópia das notificações?

O CERT.br é responsável por facilitar/coordenar as ações entre *sites*, no caso de incidentes de segurança em computadores envolvendo redes conectadas à Internet brasileira. O CERT.br também mantém estatísticas sobre os incidentes a ele reportados e desenvolve documentação de apoio para usuários e administradores de redes Internet. Manter o CERT.br nas cópias das notificações de incidentes de segurança é importante para permitir que: as estatísticas geradas reflitam os incidentes ocorridos na Internet brasileira; o CERT.br escreva documentos direcionados para as necessidades dos usuários da Internet no Brasil; o CERT.br possa correlacionar dados relativos a vários incidentes, identificar ataques coordenados, novos tipos de ataques etc.

Que informações devo incluir em uma notificação de incidente?

Para que os responsáveis pela rede de onde partiu o incidente possam identificar a origem da atividade é necessário que a notificação contenha dados que permitam essa identificação. São dados essenciais a serem incluídos em uma notificação: *logs* completos; data, horário e *timezone* dos *logs* ou da ocorrência da atividade sendo notificada; dados completos do incidente ou qualquer outra informação que tenha sido utilizada para identificar a atividade.

Onde posso encontrar outras informações a respeito de notificações de incidentes?

O CERT.br mantém uma FAQ com respostas para as dúvidas mais comuns

relativas ao processo de notificação de incidentes. A FAQ está disponível em: <http://www.cert.br/docs/faq1.html>.

O que é Segurança Legal da Informação?

É a elaboração de um plano de resposta a incidentes de segurança da informação baseado nas questões de contingências legais relacionadas à crise de imagem digital, com foco no preventivo e no bom contencioso. Para isso, é elaborada uma matriz de risco legal, na qual são determinados os indicadores que irão orientar a medição dos riscos com base em situação tecnológica, situação de cultura interna, situação de contratos, situação de exposição de imagem e de mercado, situação de uso dos canais eletrônicos, entre outras.

O que é Arquitetura Legal da Informação?

É a construção da arquitetura da informação baseada em uma visão de geração de provas legais digitais capazes de garantir a validade jurídica do documento eletrônico, para fins de uso, seja em processos, seja para comprovação das relações ou obrigações realizadas, contratadas ou acordadas via eletrônica (que vai desde um *e-mail* de aprovação ou “de acordo” até um *log* de “comprar” em uma loja virtual).

O que são Políticas Digitais?

São o conjunto de políticas, textos legais e *disclaimers* necessários para a proteção do negócio no uso de TI e Canais Eletrônicos, tais como Termo Geral de Uso do *site* ou do Serviço *Online*, Política de Privacidade, Política de Segurança da Informação, Política de uso de *e-mail* por Funcionário; Política de Compartilhamento de Dados com Terceiros, Política de *e-mail* Marketing.

Como entender o conceito de privacidade no ambiente de trabalho?

O conceito de privacidade no Brasil gera uma presunção absoluta. Isso quer dizer que, se não estiver claro que o ambiente não é privativo, a interpretação da Lei Genérica é de que, portanto, é. Precisa estar delimitado expressamente. Nos ambientes corporativos, em que o monitoramento é crescente devido a questões de prevenção de segurança da informação, é fundamental estar colocado claramente na empresa que o ambiente de *e-mail* é não privativo, de modo documental e também na interface gráfica de acesso e uso da ferramenta.

O que é certificação digital?

Certificação Digital é a atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia, inserida em um Certificado Digital, o *cliente* e a Autoridade Certificadora. Pode ser usada qualquer certificação, mas a que tem presunção de fé pública é a que está instituída pela MP n. 2.200/2001, que é a estrutura de chaves públicas do ICP-Brasil e tem a função de “garantir

a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras”.

Quem emite o Certificado Digital?

O Certificado Digital é emitido por uma terceira parte de confiança denominada CA (Autoridade Certificadora). A CA age de forma semelhante a um setor de emissão de passaportes. As CAs devem tomar providências para estabelecer a identidade das pessoas ou organizações para as quais emitem certificados digitais. Depois de estabelecerem a identidade de uma organização, elas emitem um certificado que contém a chave pública da organização, por sua vez assinado com a chave privada da CA. Com a criptografia assimétrica, a troca de chaves não é problema. As chaves públicas de um indivíduo ou corporação, como o próprio nome sugere, ficam disponíveis a qualquer pessoa que queira enviar uma mensagem criptografada, endereçada a eles, mas apenas o destinatário será capaz de decifrá-la, com sua chave privada. Surge, porém, outra questão: onde e como manter tais chaves públicas? É aí que entram as entidades certificadoras ou *Certificate Authority* (CA), em inglês, que podem, numa comparação livre, ser equiparadas aos cartórios do mundo real. São elas as responsáveis por administrar as chaves públicas e, conseqüentemente, capazes de emitir certificados digitais, ou seja, um atestado de identidade de indivíduos ou corporações.

Como funciona um Certificado Digital?

Os certificados digitais possuem uma forma de assinatura eletrônica de uma instituição reconhecida por todos como confiável, que, graças à sua idoneidade, faz o papel de “Cartório Eletrônico”. Os métodos criptográficos empregados impedem que a assinatura eletrônica seja falsificada, ou que os dados do documento sejam adulterados ou copiados, tornando-o absolutamente inviolável. Garante-se, assim, por quem assina, que os dados de identificação do certificado são verdadeiros. A Certificação Digital garante os três princípios básicos da comunicação segura em ambiente de rede de computador: autenticidade, privacidade e inviolabilidade. Então, uma vez instalada em seu computador, a Certificação Digital o reconhecerá como habilitado. Da mesma forma, seu equipamento estará apto a reconhecer um *site* certificado como verdadeiro. Em outras palavras, o documento eletrônico gerado por quem possui um Certificado Digital não pode ser posteriormente refutado, sendo estabelecido um vínculo tão forte quanto o que é gerado por uma assinatura de punho em um documento em papel.

O que é proteção digital da Marca?

É a proteção jurídica de todas as manifestações da marca em formato digital, que vai desde a assinatura do *e-mail* (a marca que vai depois do “@”), o *site*, a loja virtual, a presença em *sites* parceiros ou de terceiros, os *links*, a presença em ferramen-

tas e *sites* de busca, em mídia *online* e imprensa *online*, o bloqueio de imagens e fotos de produtos, conteúdos e tudo o mais que tiver relação com a marca.

O que é Marketing Eletrônico Legal?

É o uso das boas práticas de Direito Digital na comunicação eletrônica da empresa, de maneira que possam ser usados os bancos de dados coletados *online* de clientes e usuários de modo ético e legal, sem riscos de imagem para a marca ou contingências relacionadas à questão de privacidade. Isso se aplica desde um *e-mail marketing* até um formulário de cadastro no *site*, compartilhamento de conteúdos e bancos de dados com terceiros, promoções *online*, utilização de imagens na Internet, entre outros.

O que são Contratos Digitais Estruturados?

São contratos elaborados com cláusulas específicas para atender a questões de terceirização tecnológica, uso de certificação digital, *hosting*, *storage*, ou seja, tudo o que tenha relação com o uso de tecnologia no negócio.

O que é Home Office?

É o trabalho em casa em que a empresa capacita o profissional com equipamentos e acesso remoto à Internet e à rede da empresa.

Preciso de um contrato específico para oferecer o Home Office?

Sim. Esse contrato deve prever uma série de situações, abordando a segurança física do próprio equipamento, a responsabilidade do profissional no uso dele, os requisitos necessários para segurança da informação, o limite de uso para não gerar contingências trabalhistas, entre outros.

O gestor de TI é responsável por situações trabalhistas?

Sim. A documentação legal adequada é essencial para minimizar os riscos do gestor de TI relacionados a questões trabalhistas da empresa e também a responsabilidade civil junto a terceiros por danos que venham a ocorrer com o uso da tecnologia.

Quais as boas práticas para evitar problemas com o consumidor?

A principal delas é o dever de informar. A falta de informação pode ser interpretada como omissão ou negligência e é o maior fator de contingências. Essa falta de informação vai desde a ausência de data em uma imagem de produto colocada *online* até a questão da privacidade. Portanto, é imprescindível ter uma Política de Privacidade *Online* que já trate das questões de uso dos dados coletados, seu compartilhamento, retificação ou cancelamento de cadastro, além de segurança da informação. Portanto, mesmo que a empresa não seja uma loja virtual, é importante dar dicas de segurança, diferenciar a comunicação digital para fins de evitar riscos com a fraude eletrônica e o envio de falso *e-mail*, conhecido como *scam*.

O que é spam?

Spam não é conteúdo. *Spam* não é *e-mail marketing*. *Spam* é o envio de mensagem para uma base indeterminada de usuários. *Spam* não é invasão de privacidade (conceito legal), mas sim da expectativa de privacidade (conceito moral). O problema do *spam* é econômico (gratuito), tecnológico (acessibilidade), ético (mau uso dos dados), cultural (comunicação de massa *x* *trust marketing*) e legal (principalmente no tocante à abordagem fraudulenta e venda de listas).

O que é scam?

É um tipo de *spam* que utiliza abordagem enganosa, com falsa identidade e clonagem da imagem de uma marca que tenha elevada reputação, para ludibriar o destinatário e fazê-lo realizar alguma operação, seja de envio de dados cadastrais, seja de dados de conta corrente, até mesmo a abertura de anexos que possam conter vírus ou arquivo malicioso.

O que é phishing scam?

É uma modalidade especial de *scam* que utiliza técnica de engenharia social para ludibriar o destinatário, que passa seus dados por via do próprio *e-mail* ou acessando um *link*. Tem como característica fundamental a oferta de brinde, prêmio, vantagem, dinheiro, cadastro junto a órgão público, limpeza do nome do consumidor, crédito, entre outros. É de caráter fraudulento e falsifica normalmente a comunicação digital de uma marca de grande reputação para gerar confiança do usuário.

O que é boato eletrônico?

É um *e-mail* que é enviado trazendo algum tipo de notícia ou declaração que não pode ser provada e cuja origem não é da fonte em que o texto faz menção. É importante ter cuidado com esse tipo de mensagem; não é recomendável passá-la para frente, para terceiros, mesmo que amigos, tendo em vista que gera responsabilidade civil por eventuais danos que ela venha a causar, para quem a transmite e para a empresa que assinar o *e-mail*.

O que é computer forensics?

Segundo a definição usada pelo FBI, é "*Ciência para adquirir, preservar, obter e apresentar dados que foram processados eletronicamente e armazenados em um dispositivo de computador*".

O que é CRM Legal?

É a capacidade de construir bancos de dados que possam realmente ser utilizados sem riscos de imagem, financeiros ou legais para a marca. O uso adequado dos canais eletrônicos e dos dados permite maior fidelização (é importante ter padrão de comportamento e evitar desvio de conduta).

O que é uma Auditoria Legal-Digital?

É a realização de uma revisão completa dos ambientes eletrônicos da empresa

para fins de identificar e sanar vulnerabilidades e contingências com o foco na gestão legal do risco digital.

Como uma pessoa pode ser punida pelo mau uso da Internet?

Nossas leis atuais cobrem os problemas da Internet, porque tratam de condutas e não de meios. Se a pessoa falar de outra de modo ofensivo, pode estar cometendo o crime de injúria ou o de difamação, que são crimes contra a honra, e não importa se é oral, por escrito em um papel, em um *e-mail* ou em uma comunidade na Internet. Os usuários devem ter o cuidado de evitar situações ilícitas, como encaminhar boato eletrônico (difamação), participar de cassino virtual (jogo de azar), divulgar mensagens racistas, não exibir imagens obscenas, não criar comunidades que utilizam imagem e nome de marcas etc. Esses atos podem ser punidos com prisão, multa ou indenização à pessoa agredida.

Como exibir conteúdos no site sem infringir direitos autorais?

O primeiro passo é solicitar ao titular do conteúdo uma autorização para a publicação em sua página. Esclareça os motivos da solicitação e respeite a decisão do autor. Caso não seja possível entrar em contato com o responsável, verifique se o material possui alguma observação expondo as condições de publicação (como a necessidade de citar a fonte ou o *link* para o site do titular ou, até mesmo, pagamento de alguma taxa). Novamente, siga todas as condições impostas. Pelo princípio legal do Uso Justo, também é autorizada a reprodução de pequenos trechos da obra quando esta for utilizada para fins não comerciais.

Posso montar um blog/comunidade contra uma marca?

Existem vários meios de expressar sua insatisfação com determinado produto. Você pode entrar em contato com o SAC da empresa, procurar as entidades de defesa do consumidor ou até mesmo sites especializados, como o www.ivox.com.br, o www.reclameaqui.com.br, o www.ebit.com.br. O que não pode ser feito é utilizar indevidamente as marcas para denegri-las. Uso de marca não autorizado é infração legal. O direito de um vai até onde começa o direito do outro. Isso vale para tudo no ordenamento jurídico. Há uma harmonia, um equilíbrio, no qual os limites são dados entre o direito à privacidade, que limita o direito de liberdade de expressão, que por sua vez é limitado ao direito de proteção da imagem e da honra, e o direito do consumidor, que por sua vez é limitado pelo direito autoral, e assim por diante.

O que fazer quando um site agride minha marca?

O primeiro passo é a notificação extrajudicial do detentor do site e dos participantes que colaboram para a agressão da marca. A notificação deve conceder um prazo razoável para que todo o conteúdo seja indisponibilizado. Se a solicitação não for atendida, é necessária intervenção judicial, obrigando a retirada da página e o pagamento de multas, bem como indenização por danos morais e materiais.

Minha empresa pode tomar decisões sobre a minha carreira, baseada no que eu posto nas redes sociais?

Sim, pois o que está na rede social é público. As empresas podem checar informações nas redes sociais que você participa. Então observe se a sua conduta contribui ou prejudica sua reputação digital. Seu comportamento *online* pode ser determinante na hora da contratação ou promoção.

Como usar as redes sociais a favor da minha carreira? E o que pode depor contra ela?

O pressuposto da rede social é a transparência. Por isso, é importante passar informações pertinentes no perfil pessoal. O excesso de exposição íntima gera problemas. Já a exposição de pensamentos, textos e ideias sempre trazem retorno positivo. Também é de suma importância evitar palavras de baixo calão ou comentários sobre a rotina de trabalho.

Qual a importância do Facebook, Twitter, YouTube, entre outros canais para os consumidores?

Na sociedade da informação, isso demonstra preocupação da empresa em se aproximar e ouvir seu público. É uma forma de se mostrar acessível e disposta a dialogar, o que é essencial para as marcas. O canal aberto para o diálogo é de extrema importância na era da comunicação digital. Nas redes sociais, tudo é rápido. Nem sempre dá tempo de aprovar tudo com a área jurídica da empresa.

Como equilibrar essa agilidade com a verificação de questões legais, que pode ser demorada?

A rede social amplia o raio de alcance de um incidente, que pode tomar proporções inimagináveis. Dessa forma, o ideal é criar um canal de emergências com o jurídico da empresa. Com isso, os casos relacionados às redes podem ser tratados com urgência máxima ou em até 48 horas após o primeiro contato do consumidor.

O que as empresas devem evitar nas redes sociais?

Não é recomendável utilizar um perfil de pessoa física para representar a empresa, mesmo que seja o do presidente. O tratamento e o atendimento ao público devem ser realizados por um canal oficial da empresa. Também é importante ressaltar que haja interação e resposta ao público sempre que solicitado se o seu propósito na rede social for de relacionamento ou atendimento.

O que é a "blindagem legal" que o Social Media Legal propõe às empresas?

A blindagem legal compreende o trabalho de proteção jurídica da presença da marca nas redes sociais, seja no âmbito dos perfis oficiais, seja na verificação e no monitoramento do que aparece da marca em outros perfis (funcionários, clientes, parceiros, terceiros). O trabalho tem foco preventivo, apoia a criação e o planejamento desde a montagem da estratégia de redes sociais até a própria

implementação, com validação do conteúdo que irá ao ar. É essencial participar das redes sociais de forma sustentável e em conformidade legal, e é necessário que haja cuidado com o uso da marca, devendo-se observar os termos de uso das próprias redes sociais.

A empresa, quando participar de redes sociais, deve dar muita atenção ao conteúdo (próprio, de terceiros e em colaboração), bem como estabelecer regras claras por meio de políticas para tratar questões de privacidade, segurança da informação, direitos autorais, direitos de imagem.

O *Social Media Legal* se encarrega da elaboração da documentação e da orientação sobre a guarda de provas eletrônicas.

Se a intenção da empresa é ter um "Social SAC", ou seja, atender aos consumidores nesse ambiente, ainda, o *Social Media Legal* elabora o estudo de cenários para geração das respostas, com apoio na redação dos *scripts* (textos) já juridicamente corretos. Bem como está previsto o apoio para a realização de ações promocionais em redes sociais e para orientação para equipes internas das corporações sobre postura em redes sociais, bem como gestão de informações e uso dos conteúdos nesses ambientes. É um trabalho completo para preparar a empresa para fazer uso das redes sociais sem riscos legais.

Quais são os erros mais comuns que as empresas cometem nas redes sociais e na Internet em geral, que podem lhes trazer problemas legais no futuro?

Há situações em que as empresas utilizam perfis pessoais, de colaboradores, ou mesmo de integrantes da presidência, conselho ou diretoria para atender às solicitações de consumidores e isso é errado. O ideal tratamento e atendimento ao público deve acontecer sempre por meio de um canal oficial da corporação. Este canal oficial pode adotar um *avatar*, personificado na pessoa de um porta-voz (que pode ser o presidente), mas o registro do perfil tem que estar em nome da pessoa jurídica e não de pessoa física.

Outro erro comum é deixar de responder às solicitações dos internautas. Para as redes sociais, demorar para responder ou, pior, deixar as pessoas sem resposta pode gerar um incidente com proporções desastrosas.

Outro erro é monitorar apenas aquilo que é postado pelo público no perfil da empresa. É interessante que a empresa monitore o ambiente social de maneira geral, uma vez que muitas reclamações são postadas pelos consumidores nos seus próprios perfis.

Também é importante inserir referências de tempo para o horário de atendimento, principalmente no caso de empresas que utilizam o "Social SAC", que é o atendimento via redes sociais. A não informação sempre traz problemas em redes sociais, uma vez que o público busca e entende que, por intermédio desse canal, receberá respostas imediatas.

O uso de imagens e músicas também deve ser tratado com bastante cautela pela empresa.

O direito digital ainda é pouco conhecido das empresas?

Atualmente já é mais conhecido, em especial pelas grandes empresas. Diante do crescimento do acesso à Internet e ferramentas digitais como um todo, como o crescimento do uso de dispositivos móveis e o uso das redes sociais, fizeram com que as empresas passassem a considerar o direito digital como fundamental, bem como o apoio de um advogado com mais conhecimento tecnológico. Podemos dizer que a necessidade de inovação, a maior produção de conteúdo e a preocupação com segurança da informação fizeram com que o Direito Digital se tornasse uma disciplina obrigatória para gestores.

Como funciona a auditoria de marcas nas redes sociais?

Essa auditoria envolve uma varredura completa pela Internet para ver o que aparece sobre a marca que, então, é mapeada e separada em presença positiva, presença neutra, presença negativa e presença com riscos jurídicos. Com base nesse relatório, recomendam-se as ações. Também podemos medir o valor da marca digital: isso tem sido solicitado em processos de avaliação de ativos intangíveis para fusões e aquisições.

Existe hoje uma legislação para o uso das redes sociais?

Não há legislação específica para uso das redes sociais. No entanto, já há jurisprudência relacionada a ações e comportamentos na *web* que englobam inclusive redes sociais. A lei do mundo real se aplica para o mundo digital, então temos que considerar o que já está previsto em especial no Código Civil, no Código Penal, Código de Defesa do Consumidor, na Lei de Direitos Autorais, entre outras. O ideal é que as empresas criem manuais de conduta em redes sociais, inclusive para uso de seus colaboradores, a fim de evitar incidentes.

Que precauções uma empresa deve ter ao lançar, por exemplo, um concurso cultural na web?

Os concursos culturais, artísticos e recreativos não precisam ser previamente autorizados. Porém, as mecânicas desse tipo de ação devem ser guiadas pelos limites legais, tais como:

- Insubordinação a qualquer modalidade de sorte ou pagamento por parte dos participantes;
- Desvinculação dos participantes à aquisição ou uso de qualquer bem, direito ou serviço;
- O critério de aferição do vencedor deve ser a apuração do mérito dos participantes;
- Os dados cadastrais dos participantes apenas podem ser coletados com o objetivo de identificá-los e localizá-los e não para formação de bancos de dados;

• Vedação à divulgação ostensiva da imagem da empresa promotora, como ocorre nas modalidades sorteio, concurso e vale-brinde e respectivas assemelhadas.

Além desses tópicos, é essencial que a empresa faça uma ação em redes sociais e conheça as políticas e termos de uso de cada uma da qual for participar, porém não apenas aquelas relacionadas ao que pode ou não fazer, mas também como fazer. No *Facebook*, por exemplo, uma ação deve ser realizada por meio de um aplicativo de terceiros e não dentro da própria plataforma do *Facebook*. A equipe que for desenvolver os sistemas do aplicativo deve prever os riscos de uma quantidade muito grande de acesso, que, se for o caso, pode causar ou a queda do aplicativo ou mesmo a sua retirada, sem aviso prévio, do ar pelo próprio *Facebook*, que pode considerá-lo *spam*.

O que pode configurar o cyberbullying?

O uso de imagem não autorizada de colega (foto ou vídeo) na *web* associada a conteúdo ofensivo ou vexatório, que exponha parte do corpo do mesmo com o objetivo de ridicularizar (ex.: nariz e chamar de narigudo, orelha e chamar de orelha de abano, entre outros), bem como associar o nome de pessoa (colega, professor, terceiro) com bichos (por uso de imagem, som, outros efeitos), com o objetivo de expor a pessoa publicamente a constrangimento; ou redigir conteúdo relacionado a alguma pessoa (seja colega, professor, um terceiro) em tom agressivo, de ódio, de ameaça, discriminação, perseguição, falar mal ou denegrir a família da pessoa e do seu contexto social; ou incitar a prática de violência de uma ou mais pessoas contra uma pessoa especificamente (basta a menção de detalhes que possam gerar a identificação da mesma, mesmo que não haja citação do nome, que já configura).

Quais os principais cuidados ao usar a rede?

Alguns cuidados simples já ajudam a evitar grandes problemas. Por exemplo:

- Nunca revele senhas, elas são pessoais e intransferíveis.
- Evite o excesso de exposição na rede. Tome muito cuidado e avalie se realmente é necessário publicar suas informações pessoais, como data de nascimento, telefone, endereço, bem como outras relacionadas à sua rotina diária. Pessoas mal-intencionadas ou até criminosos podem se valer dessas informações para colocar a sua segurança em risco.
- Procure checar a fonte da informação divulgada e sempre respeite os direitos autorais, caso resolva utilizá-la (cite a fonte).
- Evite abrir arquivos de estranhos. Procure sempre passar antivírus antes de abrir qualquer arquivo. Assim evita danos ao seu computador e até mesmo mitiga o risco de seu equipamento se tornar uma máquina zumbi.
- Escolha bem as comunidades de que irá participar e evite aquelas que possam prejudicar sua imagem e reputação.

Como qualificar um crime digital?

De forma resumida, podemos dizer que os Crimes Digitais podem alcançar tanto aqueles que servem como meio, difamação em redes sociais, estelionato com uso de *e-mails* falsos, ou como fim, com os exemplos recentes de invasão a sistemas ou acesso não autorizado a dados.

Quais são os principais cuidados que os profissionais devem ter ao postar comentários pessoais nas redes sociais?

Basicamente, manifeste seu pensamento de forma responsável, respeitosa e educada. Procure não misturar sua vida pessoal com a profissional, logo, não divulgue informações do seu trabalho, de cliente, ou até mesmo da rotina de sua empresa. Isso evita que você quebre qualquer compromisso de confidencialidade, seja ele contratual ou decorrente da sua profissão.

No caso de opiniões expressas em um blog e uso indevido de material sem citação de fonte, ferindo direitos autorais, quais são as punições cabíveis?

O desrespeito aos direitos autorais é capitulado pelo art. 184 do Código Penal, com pena de detenção de 3 meses a 1 ano, ou multa.

As opiniões expressadas, caso constituírem ato ilícito, poderão ser punidas na forma de responsabilização civil por danos morais, por exemplo, ficando a cargo do juiz do caso a quantificação da multa, levando em consideração, dentre outros quesitos, a extensão do dano, a gravidade das ofensas, a capacidade de pagar do agressor e necessidade de recebimento pela vítima.

Como a legislação brasileira e os profissionais de direito estão se preparando para esses casos?

A legislação possui uma defasagem de velocidade, pois não se aprimora à medida que os meios tecnológicos evoluem, por isso existe uma dificuldade para a legislação acerca desse tema.

No entanto, já estão em discussão diplomas importantes, como o Marco Civil Regulatório da Internet, a Lei de Crimes Eletrônicos e a Lei de Proteção de Dados Pessoais.

Para alcançar a atualização, muitos profissionais buscam conhecimento com especialistas em Tecnologia da Informação e Comunicação, Segurança da Informação e daqueles que combinam o conhecimento técnico e jurídico.

O que pode ser usado de prova em um caso digital, e como saber se a prova não é forjada, já que existem várias ferramentas tecnológicas de manipulação de dados e imagens?

É permitida a ampla utilização de recursos como provas, tais como *e-mails*, arquivos de vídeo, áudio, imagem e texto.

Não existe prova infalível, tanto no meio físico quanto no digital. Para confirmar a autenticidade, integralidade e veracidade de uma prova digital é necessária

uma perícia, por meio de procedimentos próprios, que pode ser convocada em um processo caso haja dúvida ou desconfiança sobre a idoneidade da prova apresentada para o julgamento do caso.

Qual o principal desafio na hora de defender um caso de Direito Digital?

O principal desafio é a identificação do autor da conduta criminosa ou que gerou o dano. Hoje, no Brasil, por exemplo, não há uma obrigação legal para os provedores armazenarem os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores, o que dificulta um processo de identificação de autoria. Outro desafio é a preservação da prova eletrônica. Temos que ser rápidos na produção das provas haja vista a perceptível volatilidade dos dados na rede. É importante também guardar-se os *logs* dos sistemas, porém nem todas as empresas se preocupam com esse arquivo.

Qual é o caminho para quem quer fazer uma denúncia ligada à exposição não autorizada de imagem ou material divulgado na Internet? Qual é a dificuldade de rastreamento nesses casos?

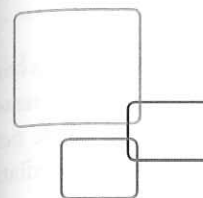
A vítima pode buscar a autoridade policial de sua localidade diretamente, ou, se preferir, pode buscar auxílio de um advogado especialista, que utilizará as vias legais para cessar o ato ilícito cometido que a expôs indevidamente.

A dificuldade para o rastreamento é detectada quando não há a devida identificação dos usuários de determinados serviços ou plataformas sem os chamados *logs* (registros computacionais) de atividade, não sendo possível determinar de onde partiu o acesso que causou danos à vítima.

Lembramos sempre da importância de registro correto das evidências e preservação adequada, para constituir de forma eficiente a prova para o caso.

Qual a importância da conscientização em massa e da conscientização pessoal na hora de acessar e publicar informações na Internet?

De maneira geral, podemos dizer que é essencial a conscientização das pessoas com relação ao uso da rede e das ferramentas tecnológicas para mitigar riscos. Isso porque a maioria dos usuários nasceu em uma era analógica e não está familiarizada com os riscos que o uso inadequado dessas ferramentas pode causar, como, por exemplo, deixar o computador do trabalho desbloqueado, com a senha de *e-mail* gravada, e alguém mandar um *e-mail* como se fosse você. Por isso acreditamos que educar é essencial.



Modelos de Documentos

Os modelos abaixo apresentados são apenas exemplificativos; dependendo da realidade e da complexidade de seu negócio, eles terão de ser adaptados.

Rodapé de *e-mail* corporativo e *e-mail* de SAC

Exemplo de avisos:

Aviso Legal

Esta mensagem pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não deve usar, copiar ou divulgar as informações nela contida ou tomar qualquer ação baseada nessas informações. Este ambiente é monitorado.

Confidencialidade e Monitoramento

Esta mensagem e quaisquer arquivos anexos podem conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, por favor, não leia, copie, repasse, imprima, guarde nem tome qualquer ação baseada nessas informações. Notifique o remetente imediatamente por *e-mail* e apague a mensagem permanentemente. Este ambiente está sendo monitorado para evitar o uso indevido de nossos sistemas. Outras informações sobre segurança e privacidade estão disponíveis em www.empresa.com.br.

Privacidade (especialmente para e-mail de marketing e SAC)

Esta mensagem e quaisquer arquivos anexos podem conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, por favor, não leia, copie, repasse, imprima, guarde nem tome qualquer ação baseada nessas informações. Notifique o remetente imediatamente por e-mail e apague a mensagem permanentemente. Aviso: não enviamos mensagens sem que tenha havido solicitação por parte do recipiente nem solicitamos dados de cartão de crédito, senhas e outras informações pessoais por e-mail. Para saber mais sobre nossa Política de Privacidade, visite www.empresa.com.br.

Indicadores para contrato de tecnologia

Item	Indicador
1.	<i>Risco de Fraude (Interna e Externa)</i>
1.1.	Vincular a observação da Política de Segurança da Informação.
1.2.	Monitoramento e registro de todas as atividades nos ambientes físicos e lógicos do Banco.
1.3.	Previsão de auditorias para verificar o cumprimento do contrato e observação das Políticas Internas da Empresa pela Contratada.
1.4.	Segregação de funções para evitar que a Contratada tenha capacidade de alterar os registros de monitoramento.
1.5.	Previsão de testes de conformidade e vulnerabilidade para Serviços de TI e <i>software</i> .
1.6.	Obrigaç�o de implementaç�o das medidas corretivas apontadas pela Empresa.
1.7.	Estabelecer crit�rios para troca e guarda segura de informa��es (VPN, Criptografia etc.).
1.8.	Obrigar a alterar senhas padr�o de equipamentos, bem como a adotar os padr�es de seguran�a sugeridos por fabricantes e melhores pr�ticas do mercado.
2.	<i>Riscos Trabalhistas e da Seguran�a de Trabalho</i>
2.1.	A Contratada deve fornecer uniformes, EPIs b�sicos, transporte e alimenta��o aos seus empregados alocados aos servi�os.

2.2.	A Contratada deve providenciar para que todos os seus empregados alocados para os servi�os sejam registrados conforme a CLT.
2.3.	A Contratada deve a fornecer � Empresa, semestralmente e quando aplic�vel: (i) c�pia do Certificado de Regularidade do FGTS; (ii) c�pia da Certid�o Negativa de INSS e, mediante solicita��o do Banco, (a) c�pia da folha de pagamento e (b) c�pia da guia GFIP — Guia de Recolhimento do FGTS e Informa��es a Previd�ncia, com o correspondente comprovante de recolhimento de FGTS e INSS; (iii) c�pia dos termos de rescis�o de contrato ocorridos no m�s, com comprovante de pagamento das verbas rescis�rias.
2.4.	Deve ser requerido da Contratada a consolida��o de seus atos societ�rios, com suas respectivas atualiza��es e os comprovantes de regularidade junto aos �rg�os fiscalizadores.
2.5.	A Contratada deve acatar as Normas de Seguran�a do Trabalho da Empresa, se houver, bem como as Normas de Seguran�a, Higiene e Medicina do Trabalho previstas na legisla��o pertinente. Incluindo a norma t�cnica OSHAS 18.001.
2.6.	A Contratada deve pagar, como �nica empregadora, todas as remunera��es, encargos sociais e trabalhistas incidentes ou que venham a incidir sobre o custo de m�o de obra, seguro de acidentes de trabalho, tributos e contribui��es que gravem os custos dos servi�os objeto do Contrato, inclusive devendo compor o pre�o dos mesmos com os encargos relativos �s reten��es de natureza fiscal previdenci�ria previstas em lei, antecipat�rias dos recolhimentos das exa��es acima, comprovando-os perante a Empresa, da mesma forma que a regularidade de situa��o perante o INSS e o Fundo de Garantia do Tempo de Servi�o.
2.7.	A Contratada dever� providenciar a retirada imediata de qualquer empregado seu, cuja perman�ncia na �rea de execu��o dos servi�os seja considerada indesej�vel pela Empresa.
2.8.	A Contratada dever� assumir o polo passivo de qualquer reclama��o trabalhista interposta por seus empregados e requerer a exclus�o da Empresa do processo.
2.9.	A Contratada deve assumir todas as responsabilidades por quaisquer processos, procedimentos ou autua��es originadas por seus empregados em fun��o do Contrato.

2.10.	A Contratada deverá ressarcir todos os prejuízos assumidos pela Empresa em razão de seus empregados sem limitação de qualquer espécie.
3.	<i>Risco de Práticas Inadequadas</i>
3.1.	Identificar se o Contrato é típico, ou se a matéria é regulada em lei especial, ou normas técnicas observáveis pela Empresa (por exemplo, bancos) e garantir que o tratamento do Contrato é compatível com as exigências legais.
3.2.	Deve ser identificado se as partes estão adequadamente representadas na forma de seus contratos sociais.
3.3.	Deve ser identificado se a parte Contratada tem idoneidade técnica para cumprir o objeto do Contrato.
3.4.	Deve ser identificado se o Contrato pode ser considerado como de consumo ou de adesão, adotando-se as cautelas pertinentes a cada tipo contratual.
3.5.	Os Contratos não devem ter natureza emulativa ou simulativa.
3.6.	A redação do Contrato deve ser clara, precisa e sempre que possível unívoca. É recomendável a utilização de glossários de termos específicos no Contrato.
3.7.	Devem ser identificadas cláusulas abusivas qualquer que seja a parte atingida.
3.8.	Os prazos de vigência, notificação de rescisão e pagamento devem ser compatíveis com a natureza da contratação.
3.9.	As obrigações principais e acessórias das partes devem estar bem delimitadas no Contrato.
3.10.	As obrigações de sigilo e de confidencialidade recíproca e as condições de divulgação devem ser adequadamente estabelecidas.
3.11.	As partes devem dispor sobre a titularidade dos direitos de propriedade intelectual das criações decorrentes do Contrato e sua utilização após o encerramento do mesmo.
3.12.	A Contratada deverá proteger e indenizar a Empresa de qualquer reclamação relativamente à violação de Propriedade Intelectual.
3.13.	A responsabilidade pelo pagamento de todos os tributos, seguros e contribuições relativas ao objeto do Contrato devem ser clarificadas, devendo inclusive compor os preços do contrato.

3.14.	Não devem ser permitidas isenções de responsabilidade civil ou limitações que não promovam uma alocação eficiente dos riscos contratuais.
3.15.	Estabelecer a obrigação de guarda e prestação de informações para auditorias e/ou processos administrativos e judiciais.
4.	<i>Risco de Danos aos Ativos Físicos Próprios</i>
4.1.	Obrigação da Contratada de zelar pelos ativos disponibilizados para a prestação dos serviços objeto do Contrato, respondendo por danos causados por culpa ou dolo aos mesmos.
5.	<i>Risco de Interrupção do Contrato.</i>
5.1.	Exigir da Contratada a adoção de planos de contingência compatíveis com as necessidades da Empresa, podendo testá-los a qualquer tempo.
5.2.	Prever uma política consistente de <i>backup</i> e <i>disaster recovery</i> .
5.3.	Propor um modelo de gerenciamento de conflitos entre as partes que evite a proposição de medidas judiciais quando as partes puderem entrar em acordo.
5.4.	Permitir a alteração do valor do contrato por motivo superveniente previamente estabelecido.
5.5.	Obrigação de colaborar com terceiros para migração do contrato para outro fornecedor/prestador.
5.6.	Prever <i>escrow</i> de código-fonte para <i>softwares</i> específicos ou sem equivalente no mercado.
5.7.	Deve haver uma garantia de acesso aos bancos de dados e todas as demais informações da Empresa serão administradas e/ou armazenadas pela Contratada.
6.	<i>Falhas em Sistemas de TI</i>
6.1.	Prever obrigação de manutenção preventiva e corretiva dos sistemas de TI com tempo de resposta compatível com a criticidade da aplicação.
6.2.	Exigir procedimentos seguros de desenvolvimento de <i>software</i> e padrões de instalação de equipamentos.
6.3.	Exigir a substituição preventiva e programada de equipamentos e sistemas para evitar obsolescência.

6.4.	Efetuar testes de conformidade e procedimentos de homologação de sistemas antes de serem colocados em produção.
6.5.	Estabelecer prazos e condições de garantia de qualidade dos sistemas.
6.6.	O desempenho dos sistemas deve ser sempre monitorado para identificação precoce de deficiências.
6.7.	Constante avaliação do dimensionamento das necessidades permitindo o crescimento da utilização dos sistemas sem sobrecargas.
6.8.	Os prejuízos causados pelas interrupções devem ser compartilhados entre as partes.
6.9.	Períodos de manutenção e manutenção programada devem ser realizados em horários de menor atividade dos sistemas.
7.	<i>Falhas na execução, cumprimento de prazos e gerenciamento das atividades</i>
7.1.	Os contratos devem possuir gestores dentro das organizações responsáveis pela medição dos serviços e acompanhamento das atividades, incluindo análise de relatórios de desempenho e SLA.
7.2.	Todos os serviços mensuráveis devem estar cobertos por acordos de níveis de serviço, a partir de indicadores objetivos e voltados aos objetivos empresariais.
7.3.	Devem ser emitidos relatórios periódicos do acompanhamento de todos os serviços cobertos por SLA.
7.4.	As penalidades do SLA não devem ter caráter de mero abatimento pelo serviço não prestado e devem ser capazes de realmente incentivar a adequada prestação do serviço. A multa deve ser mais onerosa que a prestação regular do serviço.
7.5.	Os pagamentos devem ser atrelados ao estrito cumprimento dos serviços e/ou cronograma de entrega.

Modelos de cláusulas

Segurança da Informação

Cláusula X.1 — A CONTRATANTE poderá manter registros sobre todas as atividades relacionadas à execução do presente CONTRATO que sejam efetuadas por meio de acessos físicos ou lógicos às informações confidenciais, equipa-

mentos, *softwares*, instalações, programas-fonte e quaisquer outros ativos de informação da CONTRATANTE, com o objetivo de:

a) Apurar a observação da Norma de Segurança da Informação e do Código de Conduta aplicável ao terceirizado na execução dos serviços solicitados pela CONTRATANTE;

b) Prevenir e detectar quaisquer violações à política, às normas e aos procedimentos de segurança da informação da CONTRATANTE;

c) Determinar ocorrência de algum comprometimento dos ativos de informação da CONTRATANTE, por exemplo, perda ou modificação de dados não autorizados;

d) Identificar a divulgação e reprodução não autorizada de informações confidenciais;

e) Auditar, por si ou por terceiro contratado, as responsabilidades contratuais e extracontratuais.

Direitos Autorais e Propriedade Intelectual (Contrato de Prestação de Serviços de Tecnologia)

Cláusula X.1 — Todos os direitos de propriedade dos resultados dos trabalhos realizados de acordo com o presente contrato serão de propriedade exclusiva da CONTRATANTE, bem como assim todo e qualquer conhecimento gerado. Portanto, os documentos, *know-how*, projetos, esquemas, *softwares*, código-fonte, entre outros itens produzidos durante o projeto, pertencerão única e exclusivamente à CONTRATANTE, podendo ser livremente transmitidos às demais empresas do grupo econômico desta, sendo os trabalhos tidos como obra sob encomenda.

Cláusula X.2 — A propriedade da CONTRATANTE sobre os produtos dos serviços a serem desenvolvidos por força deste contrato será plena e não se sujeitará a qualquer limitação de tempo, número de cópias ou localidade. A CONTRATANTE poderá usar os referidos produtos de todas as formas, inclusive para cópia, alteração, cessão, licenciamento ou venda, independentemente de qualquer autorização da CONTRATADA.

Cláusula X.3 — Em decorrência do disposto nesta Cláusula, fica vedada à CONTRATADA qualquer possibilidade de reprodução, cessão a qualquer título e comercialização dos referidos produtos, pois tais prerrogativas são exclusivas da CONTRATANTE, não cabendo à CONTRATADA qualquer participação em negócios realizados entre a CONTRATANTE e terceiros.

Direitos Autorais e Propriedade Intelectual (Contrato de Desenvolvimento de Software)

Cláusula X.1 — A CONTRATADA, por força do presente contrato, irá desenvolver *softwares* para a CONTRATANTE, sob encomenda. Deste modo, a CONTRATANTE será a titular de todos os direitos autorais, intelectuais e patrimoniais sobre referido *software*, o qual, inclusive, será registrado pela CONTRATANTE junto ao Instituto Nacional da Propriedade Industrial (INPI), órgão do Ministério da Indústria e do Comércio Exterior, na Divisão de Contratos de Uso de Marca e Registro de programa de Computador (DIMAPRO), o que conferirá à CONTRATANTE exclusividade na produção, uso e comercialização do *software*.

Cláusula X.2 — A CONTRATADA, na pessoa de seu representante legal, declara expressamente estar alienando à CONTRATANTE todos os direitos autorais, intelectuais e patrimoniais, sobre o *software*, comprometendo-se a fornecer à CONTRATANTE todos os documentos necessários ao registro do mesmo no INPI, bem como autoriza previamente por este ato, de maneira irrevogável, a CONTRATANTE a promover quaisquer reparos, atualizações e derivações no *software* criado em decorrência deste contrato.

Cláusula X.3 — A CONTRATADA garante que os conteúdos a serem desenvolvidos no âmbito deste contrato não infringem qualquer marca, patente, direito autoral, segredo comercial ou quaisquer outros direitos proprietários.

Atualização Tecnológica (Contratos de Licença de Software)

Cláusula X.1 — A CONTRATADA deverá, durante toda a vigência do presente contrato, disponibilizar à CONTRATANTE, mediante prévio aviso, novas versões (*releases*) do *software* licenciado, sem ônus para a CONTRATANTE.

Cláusula X.2 — As substituições de versões antigas por novas versões liberadas pela CONTRATADA, independentemente do motivo, serão de inteira responsabilidade da CONTRATADA.

Cláusula X.3 — Sempre que uma nova versão do *software* licenciado for disponibilizada, a CONTRATADA iniciará o processo de testes, com o acompanhamento de usuários nas validações, treinando-os nas novas funcionalidades, e finalizará com a transferência da versão de testes para a versão final de produção.

Cláusula X.4 — A CONTRATADA deverá, durante toda a vigência do presente contrato, disponibilizar à CONTRATANTE as atualizações legais ou compulsórias do *software* licenciado, ou seja, aquelas necessárias para manter atualizadas as funções existentes no *software* com relação às variáveis alteradas por legislação ou quaisquer outras causas externas de caráter e por determinação governamental.

Assistência na transferência ou transição

Cláusula X.1 — A CONTRATANTE obterá assistência da CONTRATADA na transferência ou transição dos Serviços para a própria CONTRATANTE, suas Afiliadas ou um Terceiro quando da rescisão ou expiração deste Contrato (Assistência na Transferência ou Transição), mediante solicitação por escrito da CONTRATANTE à CONTRATADA, que prestará essa Assistência na Transferência ou Transição à CONTRATANTE, na medida em que a CONTRATADA:

a) possa prestar essa Assistência na Transferência ou Transição solicitada empregando seus recursos então existentes, destinados exclusivamente à prestação dos Serviços sob este Contrato, até a expiração ou rescisão deste Contrato; e

b) concorde em prestar a Assistência na Transferência ou Transição, pelo período de tempo solicitado pela CONTRATANTE, período este que não será superior a seis meses após a Data de Expiração ou rescisão deste Contrato (o Período de Assistência na Transferência ou Transição).

Cláusula X.2 — Durante o Período de Assistência na Transferência ou Transição, a CONTRATADA concederá à CONTRATANTE, a suas Afiliadas e a seus Terceiros, conforme necessário, razoável acesso às Máquinas e ao *Software*, desde que:

a) esse acesso não interfira na capacidade da CONTRATADA de prestar os Serviços ou a Assistência na Transferência ou Transição; e

b) esses Terceiros e as Afiliadas da CONTRATANTE cumpram as exigências de segurança e confidencialidade da CONTRATADA.

Cláusula X.3 — A CONTRATADA arcará com todos os custos e despesas da referida Assistência na Transferência ou Transição, na hipótese de rescisão ou rescisão contratual por sua culpa.

Resilição e Rescisão Contratual

Cláusula X.1 — O presente Contrato poderá ser resilido a qualquer tempo, pela CONTRATANTE, mediante comunicação formal à outra parte, com antecedência mínima de 60 (sessenta) dias.

Cláusula X.2 — A CONTRATADA não poderá resilir unilateralmente o presente Contrato, salvo mediante comunicação formal à outra parte, com antecedência mínima de 6 (seis) meses, obrigando-se ainda a prestar os serviços necessários para transição de prestador(es) dos serviços deste Contrato.

Cláusula X.3 — Constituirá motivo para rescisão imediata do Contrato pela parte inocente, independentemente de aviso prévio, a ocorrência de qualquer das seguintes situações:

I — Inobservância, descumprimento ou cumprimento irregular das obrigações deste contrato;

II — Pedido ou instauração de processo de recuperação judicial ou extrajudicial, pedido ou decretação de falência, insolvência de qualquer uma das partes;

Cláusula de Escrow

Cláusula X.1 — Para segurança da CONTRATANTE, todas as documentações técnicas e códigos relativos ao *software*, incluindo quaisquer atualizações, deverão ser armazenados em envelopes lacrados e guardados em um local escolhido de comum acordo entre as partes, especializada em armazenamento de documentos. Os envelopes somente poderão ser abertos na ocorrência de qualquer dos eventos estipulados nesta cláusula.

Cláusula X.2 — A lacração dos envelopes deverá ser feita pela CONTRATADA, com a supervisão do CONTRATANTE.

Cláusula X.3 — Cada parte ficará com uma cópia da chave de acesso ao ambiente na qual se encontram os envelopes. Tais envelopes somente poderão ser abertos na presença de representantes de ambas as partes, em conjunto, ou pelo CONTRATANTE, caso a CONTRATADA comprovadamente:

I — Fique impossibilitada de dar continuidade ao fornecimento dos serviços necessários ao seu correto funcionamento;

II — Iniciar processo de recuperação judicial;

III — Promover concurso de credores;

III — Se sujeitar a qualquer procedimento sob a lei de falência e insolvência;

IV — Iniciar ações para liquidar seus negócios voluntariamente.

Cláusula X.4 — Na ocorrência de um dos casos previstos na cláusula anterior, a CONTRATADA concederá automaticamente à CONTRATANTE uma licença por prazo indeterminado, concedendo direitos para o uso, modificação e complementação do *software* para que a CONTRATANTE possa:

I — Integrar o *software* com sistemas e programas;

II — Adequar o *software* a mudanças legais, regulamentares, de padrões industriais ou de práticas de mercado;

III — Possibilitar que o *software* permaneça atualizado;

IV — Melhorar as funcionalidades existentes no *software*; e,

V — Possibilitar que o *software* cumpra os propósitos de negócio da CONTRATANTE.

Plano de Contingência

Cláusula X.1 — A CONTRATADA, para cumprimento deste contrato, obriga-se a criar mecanismos de contingência, observando os mesmos parâmetros utilizados pela CONTRATANTE, cabendo-lhe apresentar por escrito esse Plano de Contingência, devendo testá-lo e mantê-lo atualizado semestralmente. O Plano de Contingência deverá conter a título meramente exemplificativo:

- Plano de ação para impossibilidade de acesso ao local onde os serviços objeto deste contrato estiverem sendo prestados.

- Plano de ação para impossibilidade de locomoção (exemplo: greves de transportes, inundações).

- Plano de ação para greve geral de trabalhadores ou da categoria funcional dos profissionais alocados na prestação dos serviços, inclusive da CONTRATADA, quando isso possa afetar o bom andamento dos trabalhos.

- Os procedimentos e as prioridades para ativação do plano e a especificação das atividades a serem realizadas.

- Os nomes, endereços e telefones das pessoas responsáveis pela CONTRATADA autorizadas a efetuar a ativação do Plano de Contingência.

- Os procedimentos sobre *backups* diários, semanais e mensais dos sistemas, indicando inclusive o sistema utilizado, quando aplicável.

- Os critérios e sistemas utilizados para segurança das informações dos sistemas e dados que estiverem a seu cargo.

- Forma e periodicidade dos testes de contingência e comprovantes de sua realização, inclusive de recuperação de dados e segurança de informações.

Termo de Confidencialidade

Modelo de Análise de Termo de Confidencialidade:

ITEM	CLÁUSULA	CONFORMIDADE	
1	Definição do que são consideradas informações confidenciais	() Sim	() Não
2	Suportes em que se encontram as informações confidenciais	() Sim	() Não
3	Meios de transmissão das informações confidenciais	() Sim	() Não
4	Registros sobre os acessos às informações confidenciais	() Sim	() Não

5	Utilização de criptografia e marcações de informação confidencial e restrições de acesso a estas informações	☐ Sim	☐ Não
6	Obrigações da parte receptora de não divulgar as informações confidenciais para terceiros, exceto mediante autorização por escrito da parte divulgadora ou em decorrência de ordem de natureza judicial ou administrativa	☐ Sim	☐ Não
7	Exceções às obrigações de confidencialidade	☐ Sim	☐ Não
8	Indenização por perdas e danos decorrentes da violação do termo de confidencialidade	☐ Sim	☐ Não
9	Direito de propriedade das informações confidenciais	☐ Sim	☐ Não
10	Prazo de vigência do acordo	☐ Sim	☐ Não
11	Foro de eleição	☐ Sim	☐ Não

Modelo de Termos de Acordo de Nível de Serviço

ACORDO DE NÍVEIS DE SERVIÇO (SLA)

DA DEFINIÇÃO

Cláusula X.1 — Para efeito do presente contrato, denomina-se acordo de nível de serviço ou SLA (*Service Level Agreement*) o nível de desempenho técnico do serviço prestado pela CONTRATADA como indicador de excelência técnica, cujos critérios estão a seguir estabelecidos.

DOS CRITÉRIOS

Cláusula X.1 — O nível de desempenho no atendimento de ocorrências terá como referência os seguintes critérios de severidade:

I — Urgente — Problemas em funcionalidades essenciais, problemas no processamento de dados, problemas na comunicação entre a CONTRATANTE e os seus fornecedores;

II — Alta — Diminuição da performance de qualquer dos *softwares* em decorrência de sua atualização; problema na visualização das informações transmitidas etc.;

III — Baixa — Falha de componente que não impacta no ambiente da CONTRATANTE; problemas em rotinas de integração não essenciais;

IV — Não crítica — Pequenos erros/problemas que não tenham impacto aos negócios. Exemplo: problemas de documentação, pesquisa sobre a existência de funcionalidades etc.

SEVERIDADE	Tempo Máximo de REAÇÃO à abertura do chamado	Tempo Máximo de RESOLUÇÃO do chamado	Tempo Máximo de ATENDIMENTO do chamado (REAÇÃO + RESOLUÇÃO)
URGENTE	0,5 horas	1,5 horas	2 horas
ALTA	2 horas	4 horas	6 horas
BAIXA	4 horas	8 horas	12 horas
NÃO CRÍTICA	8 horas	12 horas	20 horas

Cláusula X.2 — Nos casos de chamados classificados com as severidades “urgente” ou “alta”, o atendimento será contínuo até a sua resolução em regime 24x7x365. Os prazos para as demais severidades determinados em horas referem-se às horas úteis, ou seja, das 09:00 às 12:00 horas e das 13:00 às 18:00 horas, devendo a contagem de tempo ser interrompida ao final de cada dia útil e reiniciada no primeiro dia útil subsequente.

Cláusula X.3 — Nos casos de chamados classificados com as severidades “urgente” ou “alta”, o atendimento será contínuo até a sua resolução.

Cláusula X.4 — Caso a solução definitiva requeira um tempo maior do que o especificado na coluna “Tempo Máximo de Atendimento do Chamado”, seja devido à sua complexidade, ou por necessidade de ajustes nas configurações ou modificação de qualquer dos *softwares*, uma solução de contorno deve ser sugerida e a severidade adequada à realidade da solução definitiva.

Cláusula X.5 — Os serviços relacionados com o Sistema deverão estar disponíveis 24 (vinte e quatro) horas por dia em todos os dias da semana, admitindo-se um acordo de nível de serviço (SLA) de até 99,5% (noventa e nove e meio por cento) do tempo dentro do mês civil.

Cláusula X.6 — A CONTRATADA deverá informar à CONTRATANTE, com pelo menos 3 (três) dias de antecedência, sobre as interrupções necessárias para ajustes técnicos ou manutenção que possam causar prejuízo à operacionalidade do servidor hospedado. As referidas manutenções e interrupções deverão ocorrer, obrigatoriamente, em horários e dias de baixa atividade da CONTRATANTE, preferencialmente, entre as 24:00 e as 6:00 horas, em período não superior a 6 (seis) horas, ficando deste já acordado que nunca poderão ocorrer em datas comemorativas e nem nas suas vésperas.

Cláusula X.7 — Não são computados para o cálculo do SLA da cláusula X.5 acima:

I — Interrupção causada por falha na conexão (*link*) fornecida por operadora ou por empresa que a substitua na prestação do serviço, sem culpa da CONTRATADA;

II — As interrupções necessárias para ajustes técnicos ou manutenção que serão informadas com antecedência e se realizarão, preferencialmente, em horários noturnos, de baixo movimento.

CLÁUSULA TERCEIRA — DO DESCUMPRIMENTO DO SLA

Cláusula X.1 — A CONTRATADA ratifica o entendimento da aplicação de penalidade progressiva prevista na cláusula das penalidades disposta a seguir, nos casos de não atendimento às obrigações relativas ao SLA.

Cláusula X.2 — A medição deverá levar em consideração os itens abaixo:

INDICADOR	SLA
Disponibilidade do Sistema	99,5%
Eficácia no atendimento dos chamados de severidade URGENTE	98,0%
Eficácia no atendimento dos chamados de severidade ALTA	96,0%
Eficácia no atendimento dos chamados de severidade BAIXA	94,0%
Eficácia no atendimento dos chamados de severidade NÃO CRÍTICA	92,0%

DAS PENALIDADES

Cláusula X.1 — Caso seja identificado e comprovado que o SLA não tenha sido cumprido, a CONTRATADA ficará sujeita a uma multa de acordo com a

tabela abaixo, incidente sobre o último valor mensal pago pela CONTRATANTE, sem prejuízo desta de pleitear perdas e danos decorrentes do descumprimento do SLA:

Taxa de Disponibilidade mensal	Penalidade (%)
Maior ou igual a 99,5%	00
Maior ou igual a 99,4% e inferior a 99,5%	02
Maior ou igual a 99,2% e inferior a 99,4%	04
Maior ou igual a 99,0% e inferior a 99,2%	06
Inferior a 99,0%	08

Cláusula X.2 — Para aferição do período de interrupção será considerado o intervalo de tempo entre a abertura do chamado até o completo restabelecimento do serviço comunicado pela CONTRATADA e ratificado pela CONTRATANTE.

Cláusula X.3 — Os valores devidos a título de multa de SLA serão compensados no próximo pagamento devido pela CONTRATANTE ou, se ao final do contrato for verificada a ocorrência do descumprimento, os valores deverão ser pagos em até 15 (quinze) dias, contados a partir da comprovação do descumprimento do SLA pela CONTRATADA.

Cláusula X.4 — Fica estabelecido que apenas dará ensejo à rescisão contratual motivada o eventual descumprimento do presente SLA em taxa de indisponibilidade inferior a 95% (noventa e cinco por cento) durante um determinado mês.

DO REGISTRO DE INCIDENTES

Cláusula X.1 — A CONTRATADA deverá disponibilizar à CONTRATANTE um sistema em que seja possível registrar os chamados relativos a incidentes e que permita à CONTRATANTE registrar data, hora, categoria (tipo) de incidente, sua descrição e sua severidade. A CONTRATADA deverá registrar no sistema as ações tomadas para a solução do incidente e, mediante relatórios do sistema, deverá ser possível consultar o atendimento dos níveis de serviço estipulados neste contrato.

Cláusula X.2 — A CONTRATADA apresentará um relatório mensal à CONTRATANTE, para averiguação da qualidade do serviço e seu desempenho no cumprimento do SLA. Ambas as partes devem definir previamente qual será o profissional ou equipe responsável, pela geração e análise dos relatórios gerados, de modo a garantir a boa gestão e governança do contrato.

TERMOS DE USO E CONDIÇÕES DE NAVEGAÇÃO: PORTAL DA EMPRESA

A Empresa apresenta aqui os Termos de Uso e Condições de Navegação de seu Portal, que deve ser respeitado pelos seus visitantes e usuários, sob pena de todas as implicações da legislação em vigor.

Para os fins destes Termos de Uso, devem-se considerar as seguintes definições e descrições para seu melhor entendimento:

Antispam: Sistema que evita correspondências não desejadas, como publicidade em massa, pelo bloqueio de mensagens ou movendo-as para pasta específica.

Aplicativo *spider*: Programa desenvolvido para obter informações de modo automatizado na Internet, navegando pela *web* (teia) como se fosse uma *spider* (aranha).

Conta de Acesso: Credencial de um visitante cadastrado que permite o acesso à área restrita e às funcionalidades exclusivas, que é definida por nome de usuário e senha.

Dados Cadastrais: Conjunto de informações pessoais de um internauta de modo que o identifique, diferenciando-o dos demais, a exemplo do número do documento de identidade (RG ou RNE), cadastro de pessoa física (CPF) ou jurídica (CNPJ), endereço residencial ou comercial, sede, nome completo, entre outros.

Empresa: Denominação utilizada nestes Termos de Uso para identificar a detentora e proprietária do Portal, [RAZÃO SOCIAL DA EMPRESA], pessoa jurídica de direito privado com sede [ENDEREÇO], na cidade de [CIDADE], Estado de [ESTADO], sob o CEP [CEP] e inscrita no CNPJ sob o n. [CNPJ].

Layout: Conjunto compreendido entre aparência, *design* e fluxos do *site*.

Link: Terminologia para endereço de Internet.

Login: Nome de Usuário escolhido pelo visitante quando preenche o cadastro para acesso a funcionalidades exclusivas do Portal.

Logon: Ato de o visitante cadastrado ingressar na área restrita do Portal utilizando seu *login* e senha.

Logs: Registros de atividades do visitante efetuadas no Portal.

Portal: Designa o endereço eletrônico [ENDEREÇO] e seus subdomínios.

Senha: Conjunto de caracteres que serve como prova de identidade digital do usuário, cujo conhecimento deve ser exclusivo e único.

Site: Denominação para página de Internet.

Usuário: Visitantes que acessam a área restrita do Portal.

Visitante: Qualquer pessoa que navegar pelo Portal.

Webmastering: Compreende criação, programação, desenvolvimento, controle e disponibilidade de páginas de Internet.

1 — Acesso e Restrições de funcionalidade

1.1. Este Portal é dedicado à atividade de compra e venda ou serviço que a Empresa desempenhe. Para efetuar uma compra ou utilizar de funcionalidades exclusivas, o visitante deverá obter uma conta de acesso, por meio do procedimento de cadastro, mais detalhado em seção própria.

1.2. Não é permitido aos visitantes e usuários acessar as áreas de programação do Portal, seu banco de dados ou qualquer outro conjunto de informações que faça parte da atividade de *webmastering*, ficando sujeito quem o fizer à legislação penal brasileira e obrigado a reparar os danos que causar.

1.3. Também não é autorizado realizar ou permitir engenharia reversa, nem traduzir, decompilar, copiar, modificar, reproduzir, alugar, sublicenciar, publicar, divulgar, transmitir, emprestar, distribuir ou, de outra maneira, dispor das ferramentas de consulta deste Portal e de suas funcionalidades.

1.4. Neste Portal é proibida a utilização, de aplicativos *spider*, ou de mineração de dados, de qualquer tipo ou espécie, além de outro aqui não tipificado, mas que atue como um robô, tanto para realizar operações massificadas ou para quaisquer outras finalidades, sob aplicação da legislação penal brasileira e de reparar os danos que decorrerem desta utilização.

1.5. É ônus dos visitantes e usuários arcar com os meios necessários para navegar neste Portal, incluindo o acesso à Internet.

2 — Informações gerais sobre o *site* e seu funcionamento

2.1. Este Portal é apresentado ao público da *web* na maneira como está disponível, podendo passar por constantes aprimoramentos e atualizações, não ficando obrigada a Empresa a manter uma estrutura ou *layout*, se não por sua própria conveniência.

2.2. A Empresa envida seus esforços para a disponibilidade contínua e permanente do Portal, ficando sujeita, todavia a eventos extraordinários, como desastres naturais, falhas ou colapsos nos sistemas centrais de comunicação e

acesso à Internet ou fatos de terceiro, que fogem de sua esfera de vigilância e responsabilidade.

2.3. A Empresa não se responsabiliza por qualquer dano, prejuízo ou perda no equipamento dos visitantes e usuários causados por falhas no sistema, no servidor ou na conexão à Internet, ainda que decorrentes de condutas de terceiros, inclusive por ações de *softwares* maliciosos como vírus, cavalos de troia, e outros que possam, de algum modo, danificar o equipamento ou a conexão destes em decorrência do acesso, utilização ou navegação neste Portal, bem como a transferência de dados, arquivos, imagens, textos, áudios ou vídeos contidos no mesmo.

2.4. Os visitantes e usuários não possuem qualquer direito para exigir a disponibilidade do Portal conforme melhor lhes convém, tampouco poderão pleitear indenização ou reparação de danos em caso de este Portal permanecer fora do ar, independentemente do motivo.

2.5. A Empresa não detém qualquer responsabilidade pela navegação dos visitantes e usuários nos *links* externos contidos no Portal, sendo dever deles a leitura dos Termos de Uso e Política de Privacidade do *site* acessado e agir conforme o determinado. Caso sobrevier algum dano ou prejuízo, os visitantes e usuários serão os principais responsáveis, uma vez que a eles cabe a navegação segura, já que a Empresa apenas apontou o *link*, cabendo ao interessado a visita, ou não, ao *site*.

2.6. A Empresa não se responsabiliza pelos atos praticados por seus visitantes e usuários no ambiente oferecido pelo Portal, devendo cada um ser imputado de acordo com a qualidade do uso da plataforma.

2.7. A Empresa poderá, a seu exclusivo critério e conveniência, excluir ou suspender a conta de acesso de determinado usuário de seu Portal, em virtude de suspeita de inexistência de informações ou prática criminosa de algum ato. Essa faculdade não exime os visitantes e usuários de fornecer sempre os dados verdadeiros e praticar condutas que coadunem com o propósito de existência do Portal e de seu cadastro nele.

3 — Cadastro dos internautas no *website*

3.1. Se desejar utilizar suas funcionalidades exclusivas ou realizar uma compra, o visitante deverá efetuar cadastro no presente Portal, fornecendo seus dados pessoais conforme requisitado e adotando uma senha forte para sua identificação e autenticação, sendo criada, ao fim do procedimento, uma conta de acesso.

3.1.1. Quando o internauta realiza o cadastro neste Portal, deve fornecer somente informações fiéis e verdadeiras, comprometendo-se, a partir de então, a manter seus dados sempre atualizados, sob pena de responder civil e criminalmente, além de arcar com os danos ocasionados pela utilização de dados incorretos, ou de terceiros, independentemente da existência de culpa.

3.2. O cadastro no Portal é gratuito e pode ser realizado por pessoas físicas maiores de 18 anos, ou em gozo de plena capacidade civil.

3.3. Ao efetuar o cadastro, o visitante declara ter pleno conhecimento deste documento e, de igual forma, da Política de Privacidade, disponíveis em todos os *links* do Portal, pois a alegação de desconhecimento não o eximirá de eventuais responsabilidades ou despistes durante a utilização do Portal.

3.4. Sempre que entender conveniente, o usuário poderá alterar sua senha e alguns dos dados de seu cadastro por meio de recurso próprio do Portal.

4 — Comunicação da Empresa com seus visitantes e usuários

4.1. A Empresa utilizará como principais canais de comunicação com seus visitantes e usuários o *e-mail* informado durante a interação com o *site*, nas suas mais diversas modalidades, e o sistema de envio de mensagens nativo do próprio Portal.

4.1.1. A responsabilidade pelo recebimento dos comunicados é exclusiva dos visitantes e usuários, por isso é indispensável que sempre forneçam os dados corretos e precisos à Empresa, e os mantenha atualizados.

4.1.2. É igualmente de sua alçada deixar seus sistemas de *antispam* configurados de modo que não interfiram no recebimento dos comunicados e materiais da Empresa, não sendo aceitável nenhuma escusa caso não tenha tido acesso a algum *e-mail* em virtude desse bloqueio ou filtro similar.

5 — Privacidade dos visitantes e usuários no Portal da Empresa

5.1. A Empresa possui documento próprio, denominado Política de Privacidade, que regula o tratamento dado às informações de cadastro e demais informações e dados coletados neste Portal.

5.2. A Política de Privacidade é parte integrante e inseparável dos Termos de Uso e Condições de Navegação deste Portal, e pode ser acessada no *link* [endereço para a Política de Privacidade], encontrado em seu rodapé.

5.3. Caso alguma disposição da Política de Privacidade conflitar com qualquer outra do presente documento, deverá prevalecer o descrito na norma mais específica.

6 — Obrigações do Portal

6.1. A Empresa se obriga com os visitantes e seus usuários a:

6.1.1. Manter o ambiente virtual seguro, salvo por ato destrutivo de terceiro que vá além dos esforços empenhados, hipótese que não se responsabilizará por danos oriundos dessa prática danosa.

6.1.2. Preservar a funcionalidade do *site*, com *links* não quebrados, utilizando *layout* que respeita a usabilidade e navegabilidade, facilitando a navegação sempre que possível.

6.1.3. Exibir as funcionalidades de maneira clara, completa, precisa e suficiente de modo que exista a exata percepção das operações realizadas.

7 — Obrigações dos visitantes e usuários

7.1. Os visitantes e usuários se obrigam a realizar uma navegação com retidão ética, sempre respeitando as condições que regem a utilização do Portal.

7.2. Os usuários deverão cuidar do sigilo e segurança de seu *login* e *senha*, pois estas informações da conta de acesso determinam a sua identidade digital, impu-tando-lhes a autoria de todos os atos praticados em seus nomes, ainda que seja por terceiro que tenha conhecimento desses dados.

7.3. Caso ocorra algum incidente com os dados de *login* e *senha*, como furto, extravio, perda ou ainda de suspeita de quebra de sigilo empregado aos mesmos, o usuário cadastrado deve alterar sua senha e comunicar de imediato a Empresa, para evitar a ocorrência de danos que podem ser de difícil reparação.

7.4. Todo usuário que possuir conta de acesso neste Portal se obriga a manter seus dados cadastrais sempre atualizados, sob pena de responder civil e criminalmente pelos danos decorrentes da imprecisão e inexatidão das informações armazenadas.

7.5. Ao fornecer dados e informações à Empresa, os visitantes e usuários se obrigam a fazê-lo sempre com compromisso de veracidade e autenticidade, sob pena da aplicação das penas da lei, de indenizar a quem causar dano e de ter a conta de acesso do presente Portal excluída ou suspensa.

7.6. Na incidência de danos ao Portal ou a terceiros, o responsável se compromete a arcar com todas as obrigações de indenizar o sujeito lesado, não devendo a Empresa responder por tais prejuízos.

7.7. Os visitantes e usuários devem utilizar os recursos do presente Portal para as finalidades às quais foram constituídos, sob pena da aplicação das penas da lei, de indenizar a quem causar dano e de ter a conta de acesso do presente Portal excluída.

8 — Direitos autorais e propriedade intelectual do Portal

8.1. O uso comercial das expressões Empresa, como marca, nome empresarial ou nome de domínio, além dos conteúdos das telas do Portal, assim como os programas, bancos de dados, redes, arquivos que permitem que o usuário acesse sua conta são de propriedade da Empresa e estão protegidos pelas leis e tratados internacionais de direito autoral, marcas, patentes, modelos e desenhos industriais.

8.2. Ao acessar este Portal, os visitantes e usuários declaram que irão respeitar todos os direitos de propriedade intelectual e os decorrentes da proteção de marcas, patentes e/ou desenhos industriais, depositados ou registrados em nome da Empresa, bem como de todos os direitos referentes a terceiros que porventura estejam, ou estiveram, de alguma forma, disponíveis no Portal. O simples acesso ao Portal não confere a estes qualquer direito ao uso dos nomes, títulos, palavras, frases, marcas, patentes, obras literárias, artísticas, literomusicais, imagens, dados e informações, dentre outras, que nele estejam ou estiveram disponíveis.

8.3. A reprodução dos conteúdos descritos anteriormente está proibida, salvo com prévia autorização por escrito da Empresa ou caso se destinem ao uso exclusivamente pessoal e sem que em nenhuma circunstância os visitantes e usuários adquiram qualquer direito sobre os mesmos.

8.4. É permitido fazer somente o arquivo temporário deste Portal, sendo vedada sua utilização para finalidades comerciais, publicitárias ou qualquer outra que contrarie a realidade para o qual foi concebido, conforme definido neste documento. Restam igualmente proibidas a reprodução, a distribuição e a divulgação, total ou parcial, dos textos, figuras, gráficos que compõem o presente Portal, sem prévia e expressa autorização da Empresa, sendo permitida somente a impressão de cópias para uso e arquivo pessoal, sem que sejam separadas as partes que permitam dar o fiel e real entendimento de seu conteúdo e objetivo.

8.5. Os visitantes e usuários assumem toda e qualquer responsabilidade, de caráter civil e/ou criminal, pela utilização indevida das informações, textos, gráficos, marcas, obras, imagens, enfim, de todo e qualquer direito de propriedade intelectual ou industrial deste Portal.

8.6. Qualquer outro tipo de utilização de material autorizado, inclusive para fins editoriais, comerciais ou publicitários, só poderá ser feito mediante prévio e expreso consentimento da Empresa. Os visitantes e usuários estão cientes, por meio deste item, que o uso comercial não autorizado poderá incorrer em infrações cíveis e criminais, por estar infringindo a lei dos direitos autorais.

8.7. Qualquer reutilização do material autorizado deverá ser objeto de uma nova autorização da Empresa.

8.8. A autorização para utilização do material solicitado não poderá ser transferida a terceiros, mesmo que vinculados ao sujeito autorizado por alguma razão.

8.9. A utilização do material não autoriza os visitantes e usuários a expor terceiros ao ridículo, criar uma obra de caráter ilegal, difamatória, obscena ou imoral, que possa violar a moral e os bons costumes, sob pena de arcar com as penalidades aplicáveis pela legislação vigente.

8.10. Qualquer utilização não contemplada na mencionada autorização será considerada como uma violação dos direitos de autor e sujeita às sanções cabíveis na Lei n. 9.610, de 19 de fevereiro de 1998, que protege os direitos autorais no Brasil.

8.11. A eventual retirada deste Portal, em decorrência de alguma reclamação, de qualquer anúncio, artigo, vídeo, produto, serviço, notícia ou fotografia aqui reproduzidos, deverá ser sempre compreendida como uma demonstração de nossa intenção de evitar dissabores com relação a este assunto e, jamais, como reconhecimento de qualquer infração pela Empresa a direito de terceiro.

8.12. As fotos e imagens utilizadas neste Portal podem não refletir seu tamanho original ou situação atual do cenário reproduzido, sendo meramente ilustrativas.

8.13. Salvo disposição específica em contrato existente entre visitantes e usuários e a Empresa, os usuários retêm os direitos autorais dos conteúdos que criarem ou que já possuírem; contudo, quando os enviam ao Portal, concedem uma licença irrevogável, perpétua, mundial, irrestrita, isenta de *royalties* e não exclusiva de reprodução, adaptação, modificação, tradução, publicação, distribuição ou exibição no próprio Portal, possibilitando a melhor utilização da ferramenta ou ilustração de algum produto ou serviço por ele oferecido.

9 — Da loja virtual da Empresa

9.1. A Empresa disponibiliza em seu Portal um ambiente que permite a aquisição de produtos e interação de seus usuários e visitantes, com possível envio de conteúdos e realizando comentários de forma geral.

9.2. A Empresa disponibiliza em seu *site* sua Política de Troca, Entrega e Devolução de Produtos, que estabelece as regras, hipóteses e condições para que essas operações sejam realizadas com sucesso e suas instruções.

9.2.1. Ao efetuar alguma aquisição no Portal da Empresa, o usuário declara ter pleno conhecimento da referida Política e manifesta sua concordância com seus termos, comprometendo-se a cumprir com os ditames lá estabelecidos para a conclusão do negócio e a requisição de algum procedimento lá estabelecido.

9.3. No ambiente do Portal, será considerado abuso e está proibido o envio os conteúdos que configurem:

- ofensa à honra, imagem, reputação e dignidade de terceiros;
- pornografia, pedofilia, e outras modalidades de satisfação sexual;
- ódio, racismo ou discriminação de qualquer natureza;
- *bullying*, *stalking* ou qualquer outra espécie de constrangimento ilegal;
- manifesta violação a direito autoral ou direito de imagem;

- utilização de marcas, símbolos, logomarcas ou emblemas de terceiros;
- instigação ou apologia à prática de crimes, como tráfico ou uso de entorpecentes, estupro, homicídio, estelionato, dentre outros;
- atividade comercial, promocional ou que sugira o exercício atividade econômica;
- atos ilícitos em geral;
- condutas contrárias à Ordem Pública e aos Bons Costumes.

9.3.1. Se detectadas quaisquer dessas práticas, a Empresa pode, a seu exclusivo critério, excluir os conteúdos, não publicá-los ou modificá-los de forma a cessar a exibição do conteúdo vedado, a qualquer tempo, sem a necessidade de aviso prévio e sem o dever de indenização pela conduta eleita como mais adequada.

10 — Atendimento do Portal Empresa

10.1. A Empresa disponibiliza os canais para comunicação direta com seus visitantes e usuários em seu Portal, pelos *links* de contato, além dos seguintes meios:

— pelo telefone [NÚMERO DE ATENDIMENTO DA EMPRESA], que atende de segunda a sexta, das [HORÁRIO DE ATENDIMENTO];

— por endereço de *e-mail* [*e-mail* de ATENDIMENTO DA EMPRESA].

11 — Modificações destes Termos e Condições

11.1. Os presentes Termos de Uso e Condições de Navegação estão sujeitos a constante melhoria e aprimoramento. Assim, a Empresa se reserva o direito de modificar a qualquer momento, de forma unilateral, o presente documento e sua Política de Privacidade.

11.2. Ao navegar por este Portal, o usuário aceita guiar-se pelos Termos e Condições de Uso do Portal da Empresa, e pela Política de Privacidade que se encontram vigentes na data e, portanto, deve verificar os mesmos cada vez que visitar este Portal.

12 — Disposições gerais

12.1. A tolerância do eventual descumprimento de quaisquer das cláusulas e condições do presente instrumento não constituirá novação das obrigações aqui estipuladas e tampouco impedirá ou inibirá a exigibilidade das mesmas a qualquer tempo.

12.2. Este Portal tem como base o horário oficial de Brasília.

12.3. A Empresa poderá cancelar a qualquer tempo e sem prévio aviso a conta de acesso de algum usuário, não sendo devida indenização, caso tenha sido

detectada e identificada alguma prática contrária ao previsto nestes Termos de Uso ou que cause dano à Empresa ou a terceiros.

13 — Lei aplicável e jurisdição

13.1. Os Termos e Condições de Uso aqui descritos são interpretados segundo a legislação brasileira, no idioma português, sendo eleito o Foro da Comarca da cidade de XXX, estado de YYY, para dirimir qualquer litígio, questão ou dúvida superveniente, com expressa renúncia de qualquer outro, por mais privilegiado que seja.

14 — Registro

14.1. Este documento encontra-se registrado no [XXXX] Cartório de Títulos e Documentos da Comarca de [XXXX].

Atualização: [DIA] de [MÊS] de [ANO].

[RAZÃO SOCIAL DA EMPRESA].

Modelo de Política de privacidade para o portal na Internet

POLÍTICA DE PRIVACIDADE: PORTAL DA EMPRESA

Como parte integrante dos Termos de Uso e Condições de Navegação do Portal da Empresa, este documento, denominado Política de Privacidade, tem por finalidade estabelecer as regras sobre obtenção, uso e armazenamento dos dados e informações coletadas dos visitantes e usuários, além do registro de suas atividades.

1 — Definições

1.1. Para fins desta Política de Privacidade, aplicam-se as seguintes definições:

Cookies: Arquivos enviados pelo servidor do Portal para o computador dos visitantes e usuários, com a finalidade de identificar o computador e obter dados de acesso, como páginas navegadas ou *links* clicados, permitindo, desta forma, personalizar a navegação dos visitantes e usuários no Portal, de acordo com o seu perfil.

Empresa: Denominação utilizada nesta Política de Privacidade para identificar a detentora e proprietária deste Portal, [RAZÃO SOCIAL DA EMPRESA],

pessoa jurídica de direito privado com sede [ENDEREÇO], na cidade de [CIDADE], Estado de [ESTADO], sob o CEP [CEP] e inscrita no CNPJ sob o n. [CNPJ].

IP: Abreviatura de *Internet Protocol*. É um conjunto de números que identifica o computador dos visitantes e usuários na Internet.

Logs: Registros de atividades dos visitantes e usuários efetuadas no Portal.

Portal: Designa o endereço eletrônico [ENDEREÇO] e seus subdomínios.

Usuário: Visitantes que acessam a área restrita do Portal.

Visitante: Qualquer pessoa que navegar pelo Portal.

2 — Obtenção dos dados e informações

2.1. Os dados e informações serão obtidos quando os visitantes e usuários:

— Realizarem seus cadastros com o preenchimento das informações necessárias;

— Interagirem com as diversas funcionalidades existentes no Portal, fornecendo as informações voluntariamente, como na seção de fale conosco, por exemplo; ou

— Adquirirem alguns dos produtos ou serviços oferecidos.

3 — Armazenamento dos dados e informações

3.1. Todos os dados e informações coletados dos visitantes e usuários serão incorporados ao banco de dados do Portal, sendo seu responsável a [RAZÃO SOCIAL DA EMPRESA], pessoa jurídica de direito privado com sede [ENDEREÇO], na cidade de [CIDADE], Estado de [ESTADO], sob o CEP [CEP] e inscrita no CNPJ sob o n. [CNPJ].

3.2. Os dados e informações coletados estarão armazenados em ambiente seguro, observado o estado da técnica disponível, e somente poderão ser acessadas por pessoas qualificadas e autorizadas pela Empresa.

3.3. Considerando que nenhum sistema de segurança é absolutamente seguro, a Empresa se exime de quaisquer responsabilidades por eventuais danos e/ou prejuízos decorrentes de falhas, vírus ou invasões do banco de dados do Portal, salvo nos casos de dolo ou culpa pela mesma.

4 — Uso dos dados e informações

4.1. Os dados e informações coletados dos visitantes e usuários poderão ser utilizados para as seguintes finalidades:

— Responder a eventuais dúvidas e solicitações dos visitantes e usuários;

- Cumprimento de ordem legal ou judicial;
- Constituir, defender ou exercer regularmente direitos em âmbito judicial ou administrativo;
- Elaborar estatísticas gerais, para identificação do perfil dos visitantes e usuários no desenvolvimento de campanhas da Empresa;
- Garantir a segurança dos visitantes e usuários;
- Manter atualizados os cadastros dos visitantes e usuários para fins de contato por telefone, correio eletrônico, SMS, mala direta ou por outros meios de comunicação.

4.2. A base de dados formada pela Empresa mediante a coleta dos dados do Portal não será compartilhada, vendida, cedida, transferida, informada ou alugada a terceiros.

4.3. Os dados adquiridos somente poderão ser acessados por profissionais devidamente autorizados pela Empresa, respeitando a necessidade a que serão submetidos, a relevância para os objetivos do Portal e aos interesses dos visitantes e usuários, além de preservar a privacidade destes.

4.4. Caso o usuário deixar de utilizar os serviços oferecidos pelo Portal, a Empresa poderá, para fins de auditoria e preservação de direitos, permanecer com o registro de dados e informações do usuário, pelo período máximo de 5 (cinco) anos, com a faculdade de excluí-los definitivamente segundo sua conveniência.

5 — Do registro de atividades

5.1. A Empresa registrará todas as atividades efetuadas pelos visitantes e usuários no Portal, por meio de *logs*, incluindo:

- Endereço de IP;
- Ações efetuadas;
- Páginas acessadas;
- Datas e horários de cada ação ou acesso;
- *Session ID*.

5.2. Os registros mencionados no item 5.1 poderão ser utilizados pela Empresa em casos de investigação de fraudes ou de alterações indevidas em seus sistemas e cadastros.

6 — Cookies

6.1. O Portal poderá fazer o uso de *cookies*, cabendo aos visitantes e usuários configurar os seus navegadores de Internet, caso deseje bloqueá-los. Nesta hipótese, algumas funcionalidades do Portal poderão ser limitadas.

7 — Disposições Gerais

7.1. As disposições constantes desta Política de Privacidade poderão ser atualizadas ou modificadas a qualquer momento, cabendo aos visitantes e usuários verificarem-na sempre que efetuar o acesso ao Portal.

7.2. O visitante deverá entrar em contato em caso de qualquer dúvida com relação às disposições constantes desta Política de Privacidade pela Seção de Fale Conosco do Portal.

8 — Lei aplicável e jurisdição

8.1. A presente Política de Privacidade será interpretada segundo a legislação brasileira, no idioma português, sendo eleito o Foro da Comarca de XXX no Estado de YYY para dirimir qualquer litígio, questão ou dúvida superveniente, com expressa renúncia de qualquer outro, por mais privilegiado que seja.

9 — Registro

9.1 Este documento encontra-se registrado no [XXXX] Cartório de Títulos e Documentos da Comarca de [XXXX].

Atualização: [DIA] de [MÊS] de [ANO].

[RAZÃO SOCIAL DA EMPRESA].

Modelo de autorização de uso de imagem e voz

TERMO DE AUTORIZAÇÃO DE USO DE IMAGEM E SOM DA VOZ

Pelo presente instrumento,

[Nome Completo], [Nacionalidade], portador do RG n. [XXXXXXXX], [Endereço Completo], doravante denominado (a) **AUTORIZANTE**,

EMPRESA., pessoa jurídica de direito privado, inscrita no CNPJ sob o n. [CNPJ] e com sede à [ENDEREÇO], doravante denominada simplesmente **AUTORIZADA**, têm entre si, justo e acordado, celebrar o presente Termo de Autorização de Uso de Imagem e Voz que será regido pelas seguintes condições:

1. O(A) **AUTORIZANTE** permite que a **AUTORIZADA** registre sua imagem e/ou som da voz doravante denominada **GRAVAÇÃO**.

2. O(A) **AUTORIZANTE** permite ainda que a **AUTORIZADA** utilize livremente a **GRAVAÇÃO**, para divulgação dentro do *site* [SITE], promovido pela

empresa **EMPRESA**, inscrita no CNPJ sob n. [CNPJ] e suas agências parceiras. Esta autorização inclui a utilização da **GRAVAÇÃO** para fins de publicidade direta de produtos ou serviços.

3. Ambas as autorizações acima englobam o emprego de qualquer tecnologia e suporte físico e/ou digital.

4. O(A) **AUTORIZANTE** consente com a utilização que será feita da **GRAVAÇÃO**, dentro do **SITE** e que a mesma poderá ser editada e sobreposta de outros elementos gráficos, com a finalidade de demonstrar as funcionalidades das ferramentas dispostas no **SITE**. O(A) **AUTORIZANTE** consente, ainda, que a **GRAVAÇÃO** poderá ser também disponibilizada em outros *sites* da Internet, sobretudo em redes sociais.

5. A **AGÊNCIA** não será responsável por qualquer utilização que os usuários do **SITE** façam da **GRAVAÇÃO** disponibilizada no **SITE**, incluindo, mas não se limitando ao *download*, distribuição por *e-mail*, disponibilização em outros ambientes da Internet, ou a fixação e transmissão em qualquer meio ou suporte.

6. No mesmo sentido, edições ou usos de partes da **GRAVAÇÃO** são autorizados somente na forma proposta no **SITE**.

7. A presente autorização é gratuita, global e definitiva, sem limite territorial ou temporal.

E, por estarem assim acordadas, o (a) **AUTORIZANTE** e a **AUTORIZADA** firmam este termo em 2 (duas) vias de igual teor e forma, na presença das 2 (duas) testemunhas abaixo assinadas, elegendo o Foro Central da Comarca de XXX, Estado de YYY, para dirimir quaisquer questões relacionadas a este termo.

[Local], de de .

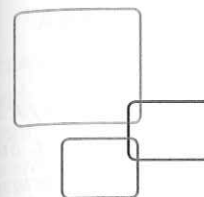
Autorizante

Autorizada

Testemunhas:

[Nome Completo]
[CPF/MF] / [RG]

[Nome Completo]
[CPF/MF] / [RG]



Jurisprudências relacionadas ao Direito Digital¹

I — INCIDENTE ELETRÔNICO — GUARDA DE PROVAS

Comentários:

Há 10 anos, havia julgados dizendo que o meio magnético ou eletrônico não era capaz de gerar prova válida, mas este entendimento mudou e evoluiu, e o Judiciário Brasileiro já entende que a prova eletrônica é hábil a comprovar a ocorrência de um fato e, se colhida corretamente, faz prova mais eficaz do que aquela colhida por outro meio.

Para o correto uso e admissibilidade da prova eletrônica em Juízo, devem ser observados os padrões técnicos de manuseio, coleta e guarda. A preservação da cadeia de custódia é essencial. As provas eletrônicas somente estarão a salvo de ser declaradas inválidas caso sejam mantidas suas integridade e autenticidade no procedimento de captura de evidências. Por isso, deve-se agir rápido para coletar a prova eletrônica, até por conta do princípio matemático chamado “ordem de volatilidade”, em que há uma tendência em um ambiente computacional de se apagar o mais antigo sobrescrevendo pelo dado mais recente. Isso justifica o pedido de liminar e a diligência urgente para busca e apreensão, quando necessário.

1. Este trabalho é de origem do escritório *Patricia Peck Pinheiro Advogados*, e sua versão eletrônica está disponível em: <<http://www.pppadvogados.com.br>>.

GUARDA DE PROVAS — RESPONSABILIDADE DA EMPRESA

“Agravamento de instrumento. Cautelar de exibição de documentos. Simples alegação de impossibilidade técnica de cumprimento da decisão que não merece prosperar. Súmula 372 STJ. Aplicabilidade. Multa diária excluída. Parcial provimento do recurso. 1. No caso dos autos, alegando violação de sua conta de e-mail, o agravado quer que a agravante lhe forneça os dados necessários para identificação dos invasores de sua conta de e-mail. 2. Haja vista a fase embrionária jurídica em relação ao assunto, ainda não se concretizaram definitivamente as posições no tocante à matéria. 3. Contudo, ainda que existam muitos nichos desconhecidos em relação à Internet, esse mesmo argumento não pode servir para justificar ou escusar a não aplicação da legislação que se tem a mão. 4. O Marco Civil da Internet no Brasil, submetido à segunda consulta pública, estabelece os direitos dos cidadãos brasileiros na Internet. 5. Ponto muito importante e positivo do Marco Civil é a forma como propõe regular os direitos e deveres relativos aos vários dados gerados pelo usuário quando navega. 6. Os registros relativos à conexão (data e hora do início e término, duração e endereço IP vinculado ao terminal para recebimento dos pacotes) terão que ser armazenados pelo provedor de acesso à Internet. 7. Em relação ao registro de acesso aos serviços de Internet (e-mails, blogs, perfil nas redes sociais etc.), o provedor não tem obrigação de armazenar os dados. Mas, se o fizer, terá que informar o usuário, discriminando o tempo de armazenamento. 8. Assim, resta claro que a simples alegação de impossibilidade técnica de cumprimento à decisão, tendo em vista não mais possuir armazenados os logs de acesso com as informações das operações realizadas no mês de setembro de 2009 não tem o condão de afastar a determinação judicial concedida nos autos da Medida Cautelar. 9. Além disso, medida não trará nenhum prejuízo ao agravante já que este estará apenas fornecendo os dados necessários para identificar os possíveis violadores da conta de e-mail do autor da ação. 10. Por outro lado, em se tratando de ação de exibição de documentos, aplica-se ao caso a S. 372, STJ. 11. Mantém-se, contudo, a decisão recorrida que determinou o fornecimento dos nomes, endereços e todos os dados que a NET tiver em seus arquivos, relativos a seus contratantes que das 22:00 horas do dia 19.09.2009 às 00:44 horas do dia 20.09.2009, se utilizaram dos IPs indicados no item 1 da petição inicial (cf. fls. 60), especificando os horários de início e fim da utilização, bem como os sites na Internet que foram acessados no curso da utilização. 12. Parcial provimento do agravo de instrumento para excluir a imposição da multa diária para caso de descumprimento” (TJRJ, Agravo de Instrumento 0013822-08.2010.8.19.00001, rel. Letícia Sardas, j. 30-6-2010).

“(…) Este controle eletrônico, mais do que os cartões picados, permite adulterações. O cartão que foi picado, picado fica, mas o controle eletrônico adulterado pode ser usado por qualquer um que possua a necessária senha de acesso ao programa. (...) Havendo prova de horas extras, como de fato há de acordo com a exordial, a fraude no controle se pressupõe, sendo absurdo imaginar que é necessário provar a fraude nos controles para se chegar à conclusão das horas extras e, pelo que dos autos consta como prova produzida oralmente emerge a veracidade da causa de pedir na íntegra (...)” (TRT15, RO 00867-2007-024-15-00-8, rel. Luiz Felipe Bruno Lobo, j. 8-5-2009).

“Passagem aérea. Compra. Cancelamento. Cartão de crédito. Cobrança. Restituição devida. Devolução em dobro. Dolo, culpa grave ou má-fé inexistentes. Operada a compra e o cancelamento da aquisição das passagens aéreas pelo próprio site da companhia, caberá à empresa provar que encaminhou à administração de cartão de crédito o cancelamento da cobrança junto ao cliente. O Direito não agracia locupletamento ou enriquecimento ilícito. Se houve o cancelamento da transação, é dever da companhia restituir o preço das passagens. A restituição em dobro é cabível em caso de dolo, culpa grave ou má-fé. Simples erro operacional ou descumprimento contratual não enseja severa punição. Recurso parcialmente provido” (TJDF, Recurso Inominado 20070610035340, rel. Luis Gustavo B. de Oliveira, publ. 17-6-2008).

“Processo civil. Revelia. Direito do consumidor. Propaganda veiculada na internet. Oferta. Vinculação do fornecedor. Inversão obrigatória do ônus da prova (arts. 30 e 38 do CDC). Danos morais não configurados. 1. A veiculação de publicidade precisa, por qualquer forma ou meio de comunicação, vincula o fornecedor, nos termos do art. 30 do CDC. 2. Não pode o fornecedor se negar a cumprir o anunciado, ao argumento de que houve equívoco na veiculação da oferta, posto que pelo princípio da boa-fé, constante da Legislação Consumerista, deve ser evitada a prática de propaganda enganosa que induza o consumidor a erro. 3. Consoante exegese do art. 38 do CDC, o ônus da prova da veracidade e correção da informação ou comunicação publicitária cabe a quem as veicula, razão por que, para fazer jus à promoção, basta ao consumidor positivar o anúncio e o seu desejo de concretizar o negócio, porquanto, segundo a diretriz emanada do dispositivo em apreço, o caso enseja inversão legal do *munus probatório*. 4. A simples recusa na realização do contrato, nos termos da propaganda anunciada, por si só, não se mostra capaz de justificar dano moral passível de compensação, haja vista não emergir ofensa aos atributos da personalidade. 5. Recurso conhecido e parcialmente provido” (TJDF, Recurso Inominado 20060410101807, rel. Sandoval Oliveira, PUBL. 19-11-2008).

PROVA LÍCITA — POSSIBILIDADE DE GRAVAÇÃO DA CONVERSA PELO INTERLOCUTOR

“Habeas corpus. Extorsão. Trancamento de inquérito policial. Provas ilícitas. Gravações, pela vítima, de conversas mantidas com o suposto infrator. Precedentes desta corte superior. Ordem denegada. 1. Inexiste divergência nesta Corte Superior quanto à legalidade da gravação feita por um dos interlocutores, tal como se dá na espécie, em que a suposta vítima do crime de extorsão realizou a gravação das conversas mantidas com o ora paciente. Precedentes. 2. Opina o MPF pela denegação da ordem. 3. Ordem denegada” (STJ, HC 87.094/SP, rel. Napoleão Nunes Maia Filho, j. 16-10-2008).

“Civil e processual. Agravo regimental no agravo de instrumento. Gravação de conversa por um dos interlocutores. Prova lícita. Desnecessidade de o julgador debater todos os argumentos levantados pela parte. Análise de matéria fático-probatória. Impossibilidade. Aplicação da Súmula 7 do STJ. Agravo não provido. (...) A gravação de conversa realizada por um dos interlocutores que se vê envolvido nos fatos é prova lícita e pode servir de elemento probatório. Precedentes. II. O Poder Judiciário, para expressar sua convicção, não está obrigado a pronunciar-se sobre todos os argumentos suscitados pelas partes, senão sobre os necessários ao deslinde da controvérsia. III. Nos termos da Súmula 7 desta Corte, a pretensão de simples reexame de prova não enseja recurso especial. IV. Agravo regimental improvido” (STJ, AgRg no Ag 962.257/MG, rel. Aldir Passarinho Junior, j. 10-6-2008).

PROVAS ELETRÔNICAS

“Responsabilidade civil subjetiva. Contrato de Subagência marítima. Fato jurídico que pode ser provado mediante presunção que não contrarie as provas dos autos. Correio eletrônico que serve de documento probatório. Atuação culposa da apelante configurada, quando não observa conhecimentos exigíveis, ocasionando a retenção da mercadoria no porto por falta de documentação adequada. Subagente que não se desincumbiu de seu ônus probatório no sentido de ter operado sem culpa. Sentença mantida. Recurso ao qual se nega provimento” (TJRJ, Apelação 0066203-29.2006.8.19.0001, rel. Antonio Iloizio B. Bastos, j. 17-8-2010).

“Execução. Título extrajudicial. Contrato de empréstimo. Cópia digitalizada. Documento original. Desnecessidade. A prova documental eletrônica, com o advento da Lei n. 11.419, de 2006, possui valor probante. A cópia digitalizada de contrato de empréstimo é documento hábil a instruir a ação executiva, não havendo neces-

sidade de se determinar a emenda da inicial, para apresentação do original do título executivo extrajudicial. Recurso provido” (TJMG, Processo 0097917-36.2010.8.13.0000, rel. Pereira da Silva, j. 8-6-2010).

“Responsabilidade civil. Protesto indevido. Inscrição junto aos órgãos de restrição creditícia. Dívida paga. Danos morais in re ipsa. Quantum. Majoração. 1. Do protesto indevido. Contexto probatório trazido aos autos revela que pelos serviços prestados em novembro de 2006, originando o boleto de n. 4.693, objeto do protesto, houve o devido pagamento pelo autor, o que, aliás, foi confirmado por mensagem eletrônica remetida por funcionária da empresa ré, não podendo o demandante ser responsabilizado pela desídia e falta de organização administrativa da empresa requerida. Assim, em tendo ocorrido o pagamento, revela-se indevido o protesto levado a efeito. 2. Dos danos morais. Em se tratando de indevida inscrição perante os órgãos de restrição de crédito, já que oriunda de dívida já paga, o dano moral está in re ipsa, pouco importando que inexistia prova nos autos quanto ao efetivo prejuízo sofrido, sendo suficiente a simples comprovação do fato. 3. Compensação. Quantum fixado na sentença, a título de compensação por danos morais, que vai majorado para R\$ 6.000,00, consideradas as circunstâncias do caso concreto. Apelo do autor parcialmente acolhido. Apelo da ré improvido” (TJRS, Apelação Cível 70034394825, rel. Paulo Antônio Kretzmann, j. 27-5-2010).

“Embargos à execução. Excesso de formalismo. Princípios da instrumentalidade do processo, celeridade e economia processual. Efeito condenatório. Prequestionamento. A declaração da nulidade pela simples nomenclatura de ‘ação de cumprimento de sentença’, além de ser um exagerado formalismo, agrediria a celeridade e a economia processual sem nenhum benefício real e legítimo às partes. A cópia da decisão extraída via Internet onde consta que foi publicada é suficiente para suprir a falta de autenticação de cópia de título executivo judicial. Deficiência perfeitamente sanável, já que a parte exequente supriu a declaração de autenticidade na impugnação aos embargos. Entendimento fundamentado nos princípios da instrumentalidade do processo, da celeridade, da economia e da efetividade na prestação jurisdicional. A ação que pretende constituir um direito ao autor e, ao mesmo tempo, condenar a ré, tem efeito anexo condenatório. Prequestionamento quanto à legislação invocada estabelecido pelas razões de decidir. Apelação improvida” (TRF4, Embargos à Execução 2009.71.05.001205-4, rel. Silvia Maria Gonçalves Goraieb, publ. 17-5-2010).

“Processual civil. Tempestividade. Greve de servidores. Paralisação das atividades. Documento extraído da Internet sem identificação da origem. Impressão de sítio não oficial. Provas inidôneas. Prova de feriado local. Ausência. Certidão da origem atestando

tempestividade. Inexistência de vinculação. 1. O recurso especial da empresa não foi conhecido por não ter se desincumbido o recorrente de utilizar provas idôneas para comprovar a paralisação das atividades do judiciário, em razão da greve de servidores, bem como por não ter realizado a prova de feriado local. 2. As portarias relativas à suspensão dos prazos foram impressas sem nenhuma identificação da procedência do documento e, em relação ao restabelecimento dos prazos, foi utilizado documento extraído do sítio da Associação dos Advogados de São Paulo, prova já afastada anteriormente nesta Corte por não ser hábil para tal fim. 3. É dever do recorrente fazer prova da existência de feriado local, para atestar a tempestividade de seu recurso, o que não fora observado nos autos. 4. Certidão lavrada por servidor público nos autos do processo, atestando apenas a tempestividade do recurso, não impede o reexame desse requisito pelo STJ. O juízo de admissibilidade realizado na instância ordinária não vincula esta instância especial. Precedentes. 5. Agravo regimental da empresa não provido. *Tributário. Prescrição. Lei Complementar n. 118/2005. Aplicação retroativa. Impossibilidade. Tese dos cinco mais cinco. Precedente do recurso especial repetitivo n. 1002932/SP.* 1. Não é possível aplicar a Lei Complementar n. 118/2005 aos casos de pagamentos indevidos realizados antes de sua vigência, pois violaria o princípio da irretroatividade. Aplica-se, ao caso, a tese dos cinco mais cinco. Precedentes. 2. Agravo regimental da Fazenda Pública não provido” (STJ, AgRg no REsp 770.786/SP, rel. Ministro Mauro Campbell Marques, j. 18-2-2010).

“Agravo regimental. Agravo de instrumento. Falta da certidão de intimação do acórdão recorrido. Informação constante em sítio do tribunal de origem na internet. Ausência de certificação. Impossibilidade. 1. Conforme a orientação dominante nesta Corte, as cópias provenientes do sítio eletrônico do Tribunal *a quo* na Internet, sem certificação de origem, não possuem fé pública. 2. Agravo regimental desprovido” (STJ, AgRg no Ag 1.198.521/SP, rel. Ministro Fernando Gonçalves, j. 9-2-2010).

“Ação de indenização. Contrato. Internet. Fidelização. Ausência de previsão contratual. Nome no cadastro dos inadimplentes. Sentença reformada. A penalidade de multa pela infidelidade contratual em caso de Internet só poderá ser cobrada se constante expressamente em contrato. A gravação de conversa sem identificação da voz não pode servir de prova. V.v. Para fixação dos danos morais devem ser levados em conta os critérios da equidade e moderação. O *quantum* da indenização devida por dano moral deve corresponder à lesão sofrida e não resultar em enriquecimento ilícito do favorecido, sendo um misto de pena e satisfação compensatória, não devendo ser inexpressiva” (TJMG, Apelação Cível 1.0024.06.223765-6/001, rel. Des. Antônio de Pádua, DOJ 10-2-2009).

“Apelação cível. Indenização. Dano moral e material. Acidente de trânsito envolvendo coletivo pertencente à empresa de conglomerado empresarial. Sentença que ex-

tingue o processo por ilegitimidade passiva. Teoria da aparência. Veículo registrado em nome da empresa R.I. Ltda. Possibilidade de ingresso em juízo contra qualquer das empresas pertencentes ao conglomerado empresarial. *Site* da Internet que relaciona todas as empresas do mencionado *pool* de empresas, dentre as quais encontra-se a proprietária do veículo envolvido no evento. A propaganda conjunta para o grupo gera credibilidade pública. Acolhimento do recurso. Anulação da sentença para prosseguimento regular do feito, com citação das demais empresas relacionadas pelo autor. Provimento do recurso” (TJRJ, Apelação 2008.001.65022, rel. Des. Sidney Hartung, j. 10-2-2009).

“(…) Código Brasileiro de Trânsito. Imposição de multa. Discussão sobre existência e/ou validade da notificação de que trata o art. 281, parágrafo único, inciso II, da Lei n. 9.503/97. Suficiência da prova eletrônica da remessa da correspondência em nome do proprietário e ao endereço declarados no registro do veículo. Exegese das Súmulas 127 e 312 do Eg. STJ. Ato administrativo com presunção de legitimidade e veracidade. Suporte doutrinário. Apelação não provida neste tema específico (...)” (TJSP, Apelação 9203383-44.2003.8.26.0000, rel. Fermino Magnani Filho, j. 14-3-2011).

“Inépcia da inicial. Preliminar rejeitada por decisão de saneamento do feito da qual não se insurgiu o autor. Preclusão consumada. Preliminar afastada. Incompetência em razão da matéria. Preliminar afastada em primeiro grau através de despacho saneador. Matéria de ordem pública. Conhecimento. Alegação de competência da Vara de Família para julgamento do feito em razão da existência de união estável entre autora e réu. Pretensão inicial que não diz respeito a reconhecimento ou dissolução da sociedade conjugal. Preliminar rejeitada. *Cerceamento de defesa.* Preliminar apreciada através de decisão interlocutória. Oferecimento de agravo de instrumento pelo réu. Decisão que negou seguimento ao recurso interposto. Preclusão consumada. Preliminar afastada. *Ação de cobrança.* Empréstimo feito ao réu através de depósitos bancários. Réu revel. Alegação de tratar-se de doação que não restou comprovada. Mensagem via documento eletrônico (*e-mail*) confessando a existência da dívida, enviado à autora não impugnado em contestação. Presunção de veracidade dos fatos narrados na inicial que não foi elidida por prova em contrário. Sentença mantida. Art. 252, do RITJESP. Recurso improvido” (TJSP, Apelação 0125971-11.2008.8.26.0100, rel. Des. Ligia Araújo Bisogni, j. 14-9-2011).

“(…) Em resumo, anotada a tendência de inverter o ônus da prova, quando a hipossuficiência técnica de uma das partes dá à outra melhor condição de provar, é de se concluir, no caso, que caberia ao banco réu, administrador de cartão de crédito, o ônus de provar a higidez do seu sistema de segurança, fato positivo, ou,

em outras palavras, a boa qualidade e a eficácia dos meios de evitar fraudes, facultado ao usuário a contraprova. Não o fez. (...) Restringindo-se a instituição financeira a sustentar apenas ter sido mais uma vítima, cinge-se a controvérsia em apurar a eficácia de seu sistema de segurança. De nada lhe aproveita continuar alegando excelência em seu sistema de segurança, pois da alegação teria que passar para a prova, que efetivamente não fez. De se presumir, portanto, que em algum momento houve falha, porque os lançamentos foram efetuados em favor de pessoa desconhecida das autoras (Alex Arão — f. 22 e 226/229). Além disso, não houve prova de que seria impossível devassar a segurança do sistema. Bem presumida, pois, a culpa do banco, daí resultando o dever de reparar os prejuízos causados. EMENTA: Responsabilidade civil. Indenização. Lançamentos em conta corrente impugnados. Inversão do ônus da prova. Admissibilidade, no caso, em que cabe ao estabelecimento bancário, na administração de cartão de crédito, comprovar a higidez do seu sistema de segurança contra fraudes. Prova desconstitutiva não produzida. Ato ilícito determinado pela responsabilidade profissional da instituição financeira. Dano material devido, restrito, no entanto, aos pagamentos efetivamente realizados e comprovados. Pessoa jurídica. Dano moral não comprovado. Ausência de efeito nocivo no âmbito negocial. Pessoa física. Dano moral configurado. Comprometimento do psiquismo. Procedência parcial da ação. Recurso principal provido em parte, provido o adesivo e desprovido o agravo retido” (TJSP, Apelação 0106792-38.2006.8.26.0011, re. Des. Luiz Sabbato, j. 23-11-2011).

“(…) Terceiro, e principalmente, porque o próprio agravante afirmou, em rede social (“Facebook”) que ‘tomou posse de uma casinha no meu sítio contra a gosto de familiares’ (fls. 21 e 51), o que, e ao contrário do afirmado, não se pode reduzir a uma simples ‘brincadeira’ com amigos. (...) EMENTA: *Possessória*. Reintegração de posse em imóvel objeto de herança que beneficiou todas as partes. Evidência de posse anterior dos agravados, particularizada em escrituras públicas. Fato que afasta a incidência incondicional do disposto no art. 1.791 do Código Civil. Preenchimento do disposto no art. 917 do Cód. de Proc. Civil, particularmente em face da prova colhida na audiência de justificação. Decisão que concedeu a liminar mantida. Agravo regimental improvido” (TJSP, Agravo Regimental 0198956-79.2011.8.26.0000/50000, re. Des. José Tarciso Beraldo, j. 26-10-2011).

“(…) No caso das fotos contidas no sítio da Internet, observando que a requerida não reconheceu a alegação feita pelo autor, é preciso ver que o crédito incorretamente feito teria caracterizado dano material. Seria importante saber por quantas pessoas o sítio foi visitado e qual o prejuízo trazido ao autor, o que dependeria de prova mais elaborada e que não foi pedida por ele. Vale notar que ele não pediu, por exemplo, para se oficiar a hospedeira do sítio para informar o número

de visitantes. Nem sequer disse se algum conhecido viu as fotos e estranhou não estar creditado. É o caso de dizer que nem todos os sítios da Internet são visitados amiúde. Hoje em dia as empresas possuem sítios quase que por obrigação, cobrança de pessoas conhecidas etc. Além disso, lembrando que a requerida não reconheceu o fato alegado pelo autor, temos que as fotos, segundo alegado por ele, foram retiradas do sítio. Nem ele foi capaz de dizer por quantos dias elas teriam permanecido na rede. EMENTA: *Cerceamento de defesa*. Desacolhimento. Julgamento antecipado da lide. Desnecessidade de produção de outras provas, em razão da natureza da demanda. Processo devidamente instruído. Incidência do inc. I do art. 330 do Código de Processo Civil. Preliminar rejeitada. *Indenização por danos materiais e morais*. Fotógrafo profissional. Contrato verbal. Não pagamento integral do preço. Utilização das fotografias para fins propagandísticos sem autorização. Procedência parcial da demanda. Inconformismo. Inadmissibilidade. Dano moral. Controvérsia acerca da existência de autorização para livre utilização das fotografias. Fatos narrados na inicial negados pela requerida. Dano moral não configurado. Inteligência do art. 333, inc. I, do Código de Processo Civil. Sentença mantida. Recurso desprovido. Preliminar rejeitada e recurso desprovido” (TJSP, Apelação 9180617-26.2005.8.26.0000, rel. J.L. Mônaco da Silva, j. 30-11-2011).

2 — DESAFIOS DA MOBILIDADE — DO E-MAIL AO CELULAR CORPORATIVO

FERRAMENTAS DE TRABALHO TECNOLÓGICAS

Comentários:

As novas ferramentas tecnológicas facilitaram a comunicação entre as pessoas, mas também trouxeram inúmeras implicações, como o uso indevido do *e-mail* corporativo pelo empregado, a possibilidade de caracterização de sobreaviso e hora extra pela utilização de celulares, programas de comunicação em tempo real, dentre outros. Por isso, a importância de se ter uma norma clara sobre “mobilidade no trabalho”, regrando o uso dos dispositivos móveis, caracterizando as situações de cargo de confiança e destacando que o fato de o colaborador portar o recurso não significa que está de sobreaviso (à disposição da empresa todas as horas do dia). Há além do aspecto trabalhista, também o risco de segurança da informação no uso de mobilidade e cláusulas sobre isso devem estar presentes.

A empresa deve estar atenta ao uso do correio eletrônico que disponibiliza aos seus colaboradores, já que é responsável pelos atos deles e pela identificação de qual colaborador utilizou-se indevidamente da ferramenta para a prática de qualquer ilícito. Nesse entendimento, os Tribunais pátrios passaram a se posicionar favoráveis ao monitoramento do *e-mail* corporativo, não apenas como um direito, mas como uma obrigação legal do empregador. Inclusive, a empresa deve orientar sobre “redação corporativa de *e-mail*”, visto que é o papel timbrado digital e o excesso de coloquialismo tem gerado diversos casos de assédio moral e sexual.

Sempre que a regra não está clara, a empresa acaba respondendo. Deve-se formalizar em políticas, normas, contratos, termos de uso, inserir avisos legais eletrônicos no ambiente de uso da tecnologia. Principalmente o aviso de monitoramento.

“*Recurso de revista da reclamada. Adicional de insalubridade. Base de cálculo. Súmula vinculante 4 do Excelso STF. Suspensão liminar da Súmula 228 do TST. Declaração de inconstitucionalidade (do art. 192 da CLT) sem declaração de nulidade. Horas de sobreaviso. Uso de telefone celular.* Apesar de a OJ-SBDI-1-TST-49 referir-se a uso do BIP, o fundamento que ensejou a edição do referido verbete foi o fato de o empregado não permanecer em casa aguardando, a qualquer momento, convocação para o serviço. Ao caso dos autos, pois, aplica-se o mesmo entendimento, uma vez que o uso de telefone celular não impede que o trabalhador saia de casa

e que tenha mobilidade. Nesse contexto, o e. TRT, ao manter as horas de sobreaviso para hipótese diversa da prevista em lei, contrariou a OJ-SBDI-1-TST-49, sendo indevida a pretensão. Destaque-se que a e. Subseção 1 em Dissídios Individuais, por expressiva maioria, já decidiu pela possibilidade de conhecimento do recurso por contrariedade à OJ-SBDI-1-TST-49, na hipótese de horas de sobreaviso com utilização de aparelho celular, ao julgar o processo TST-ED-RR — 340000-09.1997.5.02.0061, redatora Min. Maria Cristina Irigoyen Peduzzi, DJ 19/09/2008. Recurso de revista conhecido e provido. *Horas extras. Compensação. Abatimento. Critério. (...) Recurso de revista do reclamante. Intervalo intrajornada. Concessão parcial. Efeitos. (...) Conclusão:* Recurso de revista conhecido e provido” (Processo RR 286000-49.2007.5.12.0055, 3ª Turma, rel. Min. Horácio Raymundo de Senna Pires, j. 23-3-2011, DEJT 1-4-2011).

“*Horas extras.* O Juízo de primeiro grau indefere o pedido de horas extras, concluindo estar o reclamante inserido na exceção do art. 62, inciso I, da CLT (fls. 238-239). Diz o recorrente estar provado nos autos o controle da jornada por parte da empresa, consoante a prova testemunhal, buscando o pagamento de horas extras (fls. 249-251). Sem razão. Ao contrário do que alega o reclamante, não está evidenciado nos autos ter, como vendedor, sofrido controle de horário. Diante da negativa do vínculo de emprego pela reclamada, não se poderia esperar a satisfação das exigências do art. 62, inciso I, da CLT, qual seja, a anotação da condição de trabalho externo na ficha de empregado e na CTPS. Assim, cabe analisar a prova existente nos autos para chegar-se à conclusão se o reclamante estava sujeito a controle de horário. Pela natureza dos serviços prestados, a toda evidência que realizados externamente. O trabalho externo que exclui a limitação de duração é aquele que confere ao obreiro liberdade para prestação dos serviços quando lhe for mais conveniente, o que se vislumbra na espécie. O representante da empresa, ao depor, refere a ocorrência de registro de horário tão somente (...) quando os produtos são transferidos para o sistema (...) — (fl. 231). Aludido registro de horário, a toda evidência, não guarda qualquer relação com controle da jornada de trabalho do autor. Ainda, a possibilidade de o gerente poder contatar o reclamante via celular ou *e-mail* não evidencia, por si só, controle de horário. A considerar, por fim, o depoimento da testemunha M.A.S.M. (fl. 232): (...) a reclamada não controla o horário ou as visitas a clientes; que há reuniões mensais na empresa, sendo que a depoente sempre participa (...) que algum vendedor sempre falta às reuniões, mas não há qualquer punição (...). Diante deste contexto, nega-se provimento” (TST, RR-175/2003-004-04-00.1, rel. Min. Vantuil Abdala, j. 7-12-2009).

“*Horas de sobreaviso. Uso de aparelho celular.* No caso dos autos, restou incontroverso que o trabalhador permanecia com o telefone celular, por meio do qual era chamado pela empresa e que somente poderia se deslocar, desde que dentro da área

metropolitana, já que tinha que atender a eventuais chamados. Não se pode conceber que um trabalhador que porta um aparelho de telefone celular para contato pelo empregador e tomada de providências durante qualquer das vinte e quatro horas do dia tenha o pleno gozo de sua liberdade de locomoção, mesmo que a mitigação desse direito verifique-se em potencial. Desse modo, está-se diante de verdadeiro regime de sobreaviso, fazendo jus o reclamante à devida compensação financeira estipulada pelo art. 244, § 2º, da CLT. Recurso de revista conhecido e provido, no particular” (TST, RR-751/2003-005-04-00.7, rel. Emmanoel Pereira, j. 28-10-2009).

“Requer a recorrente a reforma da r. sentença para que seja excluído da condenação as horas de sobreaviso, conforme Orientação Jurisprudencial 49 da SDI-1, do C. TST. O art. 244 que trata do assunto foi editado especificamente aos ferroviários, tendo sido aplicado por analogia a outras categorias funcionais. Ocorre entretanto que, à época de sua redação, não existiam como meios de comunicação equipamentos que hoje fazem parte de nosso dia a dia, sendo corriqueiro e acessível o seu uso a qualquer pessoa independentemente de condição financeira, como, por exemplo, o telefone celular (pré ou pós-pago), *pager*, *bip* e de forma mais dispendiosa a Internet, com seus inúmeros programas de comunicação *online* (videoconferência, *messenger* etc.). Desta forma, encontra hoje o legislador a necessidade de adequar o artigo *supra* à realidade em que vivemos. Prevê o art. 244, § 2º, da CLT o pagamento de sobreaviso àqueles que permanecessem aguardando em casa o chamado da empresa. ‘Art. 244. As estradas de ferro poderão ter empregados extra numerário de sobreaviso e de prontidão, para executarem serviços imprevistos ou para substituições de outros empregados que faltem à escala organizada. (Redação dada pela Lei n. 3.970, de 13-10-61, *DOU* 16-10-61, que foi revogada e depois restaurada pelo Decreto-lei n. 5, de 4-4-1966, *DOU* 5-4-1966). § 1º (...). § 2º Considera-se de ‘sobreaviso’ o empregado efetivo, que permanecer em sua própria casa, aguardando a qualquer momento o chamado para o serviço. Cada escala de ‘sobreaviso’ será, no máximo, de 24 (vinte e quatro) horas. As horas de ‘sobreaviso’, para todos os efeitos, serão contadas à razão de 1/3 (um terço) do salário normal. (Redação dada pela Lei n. 3.970, de 13-10-1961, *DOU* 16-10-1961, que foi revogada e depois restaurada pelo Decreto-lei n. 5, de 4-4-1966, *DOU* 5-4-1966)’. Considerando-se que, à época da redação do artigo *supra*, a telefonia fixa era privilégio de poucas pessoas, realmente se fazia necessário que o obreiro aguardasse, sem a possibilidade de sair de sua casa, o chamamento da empregadora. Com a telefonia móvel, fixa e todos os outros meios de comunicação, o empregado pode ser encontrado a qualquer tempo, em qualquer lugar, independentemente de estar ou não em sua casa, podendo ou não estar quer seja no convívio com sua família em momento de lazer ou mesmo laborando para outro empregador ou dispondo de seu tempo como melhor lhe aprouver. Entendo *data maxima venia* que, à exceção da Internet por meio de programas de comunicação tal como

‘videoconferência’ ou *messenger*, qualquer outro meio de comunicação para fins de caracterização de ‘horas de sobreaviso’ é imprestável, eis que nenhum deles efetivamente cerceia ou é fator impeditivo da liberdade de locomoção prevista pelo art. 244 da CLT. O próprio TST reconheceu que o uso de *bip* — que hoje já se modernizou — não caracteriza o sobreaviso, exatamente pelos motivos exposto *supra*. ‘49 — Horas extras. Uso do *bip*. Não caracterizado ‘o sobreaviso’. (Inserida em 1-2-1995. Nova redação — Res. 129/2005, *DJ* 20-4-2005). O uso do aparelho *bip* pelo empregado, por si só, não caracteriza o regime de sobreaviso, uma vez que o empregado não permanece em sua residência aguardando, a qualquer momento, convocação para o serviço’. A situação atual, conforme exposto, é totalmente diferente da época da redação do dispositivo legal, beneficiando a empresa — que com todos os meios a seu favor conta com o funcionário, pode chamá-lo quando for necessário sem a necessidade de que este permaneça dentro de casa —, caracterizando o sobreaviso e complicando a situação do obreiro, que dificilmente consegue demonstrar que estava realmente em sua residência aguardando o chamado de sua empregadora. Como consequência lógica, entendo que o sobreaviso, nos termos previstos no art. 244 CLT, cada vez mais encontrará dificuldade em sua caracterização. Em assim sendo, impõe-se a reforma da decisão de origem, eis que não restou provado que o autor efetivamente aguardava em sua residência a convocação da ré, excluindo da condenação o pagamento das horas de sobreaviso” (TST, RR 2105/2001-006-02-85.2, rel. Rosa Maria Weber Candiota da Rosa, j. 21-10-2009).

“Horas extras (...) O exercício de cargo de confiança não restou reconhecido pelo juízo de origem, porém, acertadamente, a meu ver, entendeu o julgador que o autor não estava sujeito a controle de jornada. Em depoimento pessoal, esclareceu o reclamante que ‘(...) na unidade de Canoas I e II não havia superior hierárquico ao reclamante lotado naquele local’, acrescentando que ‘eram superiores hierárquicos do reclamante o subgerente e o gerente geral, sendo que ambos eram encarregados de oito usinas hidrelétricas, aproximadamente. O subgerente e o gerente geral estavam lotados em Xavantes-SP, e o reclamante comunicava-se com eles através de *e-mail* e telefone; (...) o gerente e o subgerente fiscalizavam as obras conduzidas pelo reclamante cerca de uma a duas vezes por semana; (...) o reclamante trabalhava externamente, em campo, fora da fiscalização de horário da reclamada, mas podia ser encontrado por telefone celular (...)’ (fls. 179/181). Ora, suficiente o depoimento do autor para corroborar a conclusão do juízo de origem, posto que é evidente que não sofria efetiva fiscalização quanto ao horário cumprindo, inexistindo superior hierárquico no local de trabalho. Indevidas, portanto, as horas extras, bem como os reflexos daí decorrentes, enquadrando-se o autor na exceção prevista no art. 62, I, da CLT. Mantenho” (TST, AIRR 452/2002-036-15-40.4, rel. Min. Horácio Senna Pires, j. 24-6-2009).

“Agravado de instrumento em recurso de revista. Adicional de transferência. Súmula 126 do TST. Sobreaviso. Horas extras. Celular. Orientação Jurisprudencial 49 da SBDI-1 do TST. Da multa do art. 477 da CLT. Desfundamentado. Nega-se provimento ao Agravado de Instrumento que não logra desconstituir os fundamentos do despacho que denegou seguimento ao Recurso de Revista. Agravado de Instrumento a que se nega provimento (TST, AIRR 1391/2002-205-01-40.7, rel. Márcio Eurico Vitral Amaro, j. 10-6-2009).

*“Horas de sobreaviso. Uso do celular. Orientação Jurisprudencial n. 49 da SBDI-1. Não caracteriza sobreaviso o porte de instrumento de comunicação pelo empregado (como o uso de *bip*). Inteligência da Orientação Jurisprudencial n. 49 da SBDI-1. Recurso de Revista conhecido parcialmente e provido” (TST, RR 9.848/2000-006-09-00.1, rel. Maria Cristina Irigoyen Peduzzi, j. 13-5-2009).*

*“Horas extras. Sobreaviso. Uso do bip. Caráter obrigatório. Emergência. Solução de problemas à noite e nos sábados. Segundo a Orientação Jurisprudencial n. 49 da SBDI-1, o uso, por si só, do *bip* é insuficiente para o reconhecimento do direito às horas de sobreaviso. Não é aplicável aos casos, entretanto, em que se configure não apenas o uso, mas a explícita interferência na liberdade do trabalhador de ir e vir. Essa é a peculiaridade fática a diferenciar o caso descrito na decisão recorrida da hipótese contemplada na Orientação Jurisprudencial n. 49 da SBDI-1, pois o Reclamante era acionado à noite entre 18h e 23h, após o expediente, e, inclusive nos sábados, para resolver problemas emergenciais da empresa. Além disso, segundo o Regional, tinha a liberdade de ir e vir limitada — no que concerne a distância e dificuldade de acesso dos eventuais locais que pretenda visitar ou frequentar, ou simplesmente, estar. Honorários de advogado. Impossibilidade de exame de contrariedade às Súmulas 219 e 329 desta Corte. A conclusão exclusiva de que a condenação ao pagamento dos honorários de advogado decorreu da condição de hipossuficiência econômica do empregado não permite, por si só, reconhecer contrariadas as Súmulas 219 e 329 desta Corte, salvo se houver elementos fáticos, na decisão recorrida, a permitir que se reconheça não estar o trabalhador assistido por sindicato da categoria profissional ou simplesmente assistido por advogado particular. Recurso de revista não conhecido” (TST, RR 37791/2002-900-09-00.8, rel. Emmanoel Pereira, j. 29-4-2009).*

“Rito sumaríssimo. Recurso ordinário. Justa causa. Art. 482, b, da CLT. Burla de regras da empresa para acesso a sítios, o que era vedado. Norma regulamentar da qual o reclamante tinha conhecimento prévio. Computador e Internet, instrumentos de trabalho utilizados irregularmente, para uso pessoal. Incontinência de conduta e mau procedimento. Falta grave que está caracterizada” (TRT02, RO 01875200843102004, rel. Carlos Francisco Berardo, j. 17-2-2009).

*“O uso de aparelho de intercomunicação, a exemplo de *bip*, *pager* ou aparelho celular, pelo empregado, por si só, não caracteriza o regime de sobreaviso, uma vez que o empregado não permanece em sua residência aguardando, a qualquer momento, convocação para o serviço” Súmula TST 428. Sobreaviso (conversão da Orientação Jurisprudencial n. 49 da SBDI-1). Res. 174/2011, DEJT divulgado em 27, 30 e 31-5-2011.*

*“(…) entendo que houve violação ao direito à intimidade do obreiro. Com efeito, *e-mail* nada mais é que correio eletrônico. Ou seja, correspondência enviada pelo computador. Ainda que se utilize o computador da empresa, o endereço (eletrônico) pertence ao reclamante. Manifesta a violação de correspondência, ainda que eletrônica, fere a garantia à intimidade (Constituição Federal, art. 5º, inc. VIII)” (TRT02, RO 20000-34734-0, rel. Fernando Antonio Sampaio da Silva, j. 3-8-2000).*

*“Utilização de *e-mail* corporativo para receber e enviar material pornográfico. Conduta contrária à norma interna da empresa. Demissão por justa causa caracterizada. O uso de correio eletrônico tem se tornado cada vez mais comum nas empresas, tornando-se importante equipamento de trabalho para potencializar a consecução do serviço. E, como instrumento de trabalho, deve ser usado com parcimônia pelo empregado, o qual deve ser diligente em utilizá-lo de forma adequada, observando os fins a que destinam. A conduta do Reclamante incorreu em desrespeito à norma da empresa que expressamente proíbe o uso de seus recursos de informática para fins não profissionais, vedando expressamente sua utilização para divulgação de materiais contrários aos bons costumes. A gravidade da conduta do empregado que recebe material pornográfico e divulga para terceiros, utilizando-se de *e-mail* corporativo da empresa abala a fidúcia que deve existir nas relações de trabalho, mesmo porque pode ocasionar ato lesivo à imagem da empresa e sua responsabilização perante terceiros. Assim, restando incontroverso que o Reclamante, mesmo ciente da proibição imposta pela Reclamada, utilizou-se de *e-mail* corporativo da Reclamada para receber e divulgar material pornográfico, pois ele próprio admite tal fato, agiu a Reclamada dentro do seu poder regulamentar disciplinar em demitido por justa causa. Nego provimento. (...)” (TRT, 23ª Região, RO-0031600-92.2010.5.23.0076, rel. Des. Leila Calvo, j. 3-8-2011).*

*“Visando apurar a materialidade em questão, o *hard disc* do computador pertencente à D. foi submetido à perícia técnica, cujo laudo encontra-se encartado às fls. 205/219, onde os expertos concluíram que foram localizadas imagens pornográficas armazenadas no disco rígido na área do usuário denominado POLICIAL, bem como *links* de acesso ao mensageiro *online* denominado “eBuddy” para MSN, Yahoo, GTALK, Facebook, ICQ, MySpace e AIM (AOL), através do usuário*

'grumec@hotmail.com'. Referida prova material, aliada ao relatório de fls. 26, bem como às declarações do próprio sindicato, tanto em sede de apuração preliminar quanto no interrogatório da presente sindicância, aliadas aos depoimentos de R.C.O. às fls. 334/335, demonstram que o sindicato realmente fez uso do equipamento em questão para assuntos particulares nas ocasiões mencionadas na portaria inaugural (fls. 528) (...) *Servidor público estadual. Investigador de Polícia. Pretensão de anular a pena de suspensão imposta. Inadmissibilidade*. Processo administrativo que teve trâmite legal, assegurando ao acusado o direito ao contraditório e à ampla defesa. Sentença improcedente. Não pode o Poder Judiciário entrar no mérito do ato administrativo e, assim, não se pode sustentar a procedência do pedido, no entendimento de que as justificativas apresentadas não eram bastante para supedanejar a penalidade aplicada. Recurso desprovido" (TJSP, Apelação 0012911-36.2010.8.26.005, rel. Des. Samuel Junior, j. 31-5-2011).

USO INDEVIDO DO CORREIO ELETRÔNICO POR EMPREGADO

"Despedida por justa causa. Inexistência de abuso do direito à liberdade de expressão (art. 5º, IV, da CF). Não configura conduta capitulada no art. 482, "k", da CLT o empregado que envia *e-mail* a outros obreiros e ao próprio empregador relatando as infrações da legislação trabalhista cometidas pela empresa, desde que não represente abuso de direito à liberdade de expressão, mormente quando se considera o atraso na remuneração de férias que justificou a procedência parcial da demanda" (TRT02, RO 00752-2006-019-02-00-8, rel. Des. Adalberto Martins, j. 19-3-2009).

"Cláusula de confidencialidade. Incorre nas hipóteses de justa dispensa o empregado que conscientemente transgredir cláusula contratual que impede a retirada de documentos do âmbito da empresa sem expressa autorização, colocando em risco o sistema de segurança adotado. (...) o reclamante transgrediu o regulamento interno da empresa ao remeter para seu endereço eletrônico particular arquivos contendo o desenvolvimento de projetos de propriedade da demandada, sem autorização" (TRT02, RO, Acórdão 20090369100, rel. Ana Maria C. B. Silva, j. 12-5-2009).

"Utilização habitual de *e-mail* corporativo para envio de mensagens de cunho pessoal, ou não relacionada com o trabalho, não obstante ciência de norma interna vedando o procedimento. *Histórico*: A empresa tomou conheci-

mento que seu colaborador, no período de 21-8-2006 a 19-10-2006 (dois meses), repassou 92 (noventa e dois) *e-mails*, ao passo em que os outros 10 colegas de trabalho, no mesmo período, fizeram uso desse expediente 01 (uma) vez (cinco colegas), 02 (duas), 07 (sete) e 24 (vinte e quatro) vezes. Mesmo não se tratando de conteúdo imoral ou proibido, considerou-se que a dispensa por justa causa não feriu o princípio da ampla defesa e tão menos foi discriminatória. Logo, o pedido de reintegração no emprego não foi acolhido" (TRT04, RO, Acórdão 00007-2007-010-04-00-1, rel. Maria da Graça R. Centeno, j. 3-9-2009).

"Agravado de instrumento em recurso de revista. E-mail corporativo. Acesso pelo empregador sem a anuência do empregado. Prova ilícita não caracterizada. Consoante entendimento consolidado neste Tribunal, o *e-mail* corporativo ostenta a natureza jurídica de ferramenta de trabalho, fornecida pelo empregador ao seu empregado, motivo pelo qual deve o obreiro utilizá-lo de maneira adequada, visando à obtenção da maior eficiência nos serviços que desempenha. Dessa forma, não viola o art. 5º, X e XII, da Carta Magna a utilização, pelo empregador, do conteúdo do mencionado instrumento de trabalho, uma vez que cabe àquele que suporta os riscos da atividade produtiva zelar pelo correto uso dos meios que proporciona aos seus subordinados para o desempenho de suas funções. Não se há de cogitar, pois, em ofensa ao direito de intimidade do reclamante. Agravado de instrumento desprovido" (TST, AIRR-1640/2003-051-01-40.0, rel. Vieira de Mello Filho, j. 15-10-2008).

"Despedida por justa causa. Mau procedimento. Uso indevido de correio eletrônico. Quando se caracteriza. Prova que evidencia a utilização do *e-mail* funcional, pelo empregado, para difundir informações tendentes a denegrir a imagem da empregadora. Constitui justa causa para a despedida o uso indevido do correio eletrônico fornecido pelo empregador, não se podendo cogitar de infração ao disposto no art. 5º, XII, da CF, já que o serviço de *e-mail* é ferramenta fornecida para uso estritamente profissional. Sentença mantida" (TRT4, RO 00168-2007-203-04-00-3, rel. Flavio Portinho Sirangelo, j. 3-9-2008).

"(...) O caso em espécie é de descoberta acidental pelo empregador que a Autora cometera falta gravíssima, contrariando expresso dispositivo do contrato de trabalho, avençado por escrito, e repassava segredos comerciais da Reclamada para empresa concorrente. (...) Como assistente de importação e exportação detinha conhecimentos de segredos estratégicos e táticos da empresa. E tinha compromisso

expresso de sigilo. E de tanto não se preocupou ao ceder, sem permissão, os dados que dispunha em razão do cargo ocupado. (...) Com os fundamentos *supra* dou provimento ao apelo da Reclamada para considerar justa a demissão tendo em vista a gravidade da falta cometida. (...)” (TST, Ag. Instr. em RR 2771/2003-262-02-40, rel. Maria de Assis Calsing, j. 2-4-2008).

“*Responsabilidade civil. Ação de indenização. Divulgação e/ou retransmissão de e-mail com ofensas à honra e à dignidade dos demandantes.* Ainda que a autoria do conteúdo do *e-mail* divulgado, repassado ou retransmitido por funcionária da parte demandada, em estrita observância de ordens superiores, não tenha sido conhecida, responde a demandada por culpa no evento, considerando que contribuiu para a divulgação do seu conteúdo, ainda mais quando assumido pela demandada que a divulgação do *e-mail* se deu a partir dos seus computadores. Mensagens enviadas, encaminhadas ou remetidas pela demandada, pelos meios de comunicação eletrônica, e que contêm expressões injuriosas dirigidas aos demandantes, violam a honra dos mesmos e assegura o direito de indenização pelo dano moral causado (art. 5º, X, da Constituição Federal). Indenização não deve ser em valor ínfimo, nem tão elevada que torne desinteressante a própria inexistência do fato. Atenção às particularidades das circunstâncias fáticas e aos precedentes da Câmara, na manutenção de equivalência de valores entre lides de semelhante natureza de fato e de direito. Descabe o prequestionamento, pois o magistrado não é obrigado a responder a toda e qualquer indagação de ordem legal formulada pelo recorrente. Sentença reformada. Apelação parcialmente provida. Unânime” (TJRS, Apelação Cível 70022318711, rel. Jorge Alberto Schreiner Pestana, j. 29-5-2008).

“(...) Parece-me imperativo, a propósito, desde logo, distinguir duas situações básicas: *e-mail* particular ou pessoal do empregado e *e-mail* corporativo. No caso de *e-mail* particular ou pessoal do empregado — em provedor próprio deste, ainda que acessado louvando-se do terminal de computador do empregador —, ninguém pode exercer controle algum de conteúdo das mensagens porquanto a Constituição Federal assegura a todo cidadão não apenas o direito à privacidade e à intimidade como também o sigilo de correspondência, o que alcança qualquer forma de comunicação pessoal, ainda que virtual. É, portanto, inviolável e sagrada a comunicação de dados em *e-mail* particular. (...)”. Nesses termos, por violar os princípios constitucionais da intimidade, da privacidade e do sigilo da correspondência, reputo ilícitas as provas carreadas aos autos às fls. 65/66, 75/77, 86/92 e 98, sendo imprestáveis para demonstrar a existência de

amizade íntima entre a reclamante e a sua primeira testemunha. (...) *Documentos obtidos a partir do e-mail pessoal do empregado. Prova ilícita configurada.* Ilícitas são as provas utilizadas pelo empregador que têm como origem o *e-mail* pessoal do empregado, eis que há a violação dos princípios constitucionais da privacidade e da intimidade, bem como ao sigilo da correspondência, previstos, respectivamente, nos incisos X e XII da Constituição da República” (TRT02, Processo 02683-2008-085-02-00-4, 4ª Turma, rel. Des. Maria Isabel Cueva Moraes, j. 26-7-2011).

“(...) Ocorre que o autor simplesmente gravou, armazenou arquivos para leitura posterior, sem que se tenha cogitado, nos autos, de divulgação, por qualquer meio, tampouco de acesso a páginas de conteúdo impróprio, na Internet. Considerá-lo um perverso, como faz a ré, tem algo de inquisitorial e, pior, de um sentimento de ‘posse’ em relação à pessoa do empregado. (...) Por derradeiro, não prospera a alegação de divergência jurisprudencial, eis que as decisões transcritas às fls. 500/508 das razões de recurso de revista são inseríveis à demonstração do dissenso, porquanto inespecíficas, vez que nenhuma delas aborda a questão sob o enfoque conferido no v. acórdão recorrido, no sentido de que a conduta da reclamada denota inegável abuso do poder de despedir, o que gera nulidade da ruptura contratual, especialmente pelo fato de ter sido aplicada, liminarmente, a pena mais grave possível a empregado que não possuía qualquer restrição na ficha funcional, na medida em que o fato, incontroverso, do reclamante receber via *e-mails* mensagens de conteúdo erótico/pornográfico e armazená-las em seu disco rígido (e não em arquivos da rede da empresa), jamais poderia ser considerada infração grave, até mesmo porque ausente qualquer determinação em contrário e, também, pelo fato de que ele (reclamante) não repassava tais *e-mails* para dentro ou fora da empresa, bem como não ‘visitava’ sites de conteúdo pornográfico em seu ambiente de trabalho. Aplicabilidade da Súmula/TST 296, item I. (...)” (TST, Processo RR-1304300-75.2005.5.09.0029, rel. Min. Renato de Lacerda Paiva, j. 19-10-2011).

MONITORAMENTO DE E-MAIL CORPORATIVO — LEGALIDADE

“Primeiramente o reclamante informou que não utilizava a senha do gerente, ao passo que o informante, que era o gerente da loja, disse que o reclamante utilizava sua senha. Tal contradição demonstra o interesse do reclaman-

te em expor os fatos da forma que entendeu que melhor poderia serem vistos pelo Juízo, visando obter pronunciamento judicial a seu favor. Além disto, o procedimento investigatório se limitou a questionamentos efetuados às pessoas que foram acusadas por *e-mail* da prática de ato ilícito. É de se considerar que a existência de irregularidades no estabelecimento em que o reclamante laborava é fato que não foi negado nem pelo reclamante e nem pelo informante. O que ocorreu, entretanto, é que as investigações realizadas pela reclamada não culminaram em conclusão acerca da autoria dos atos ilícitos. Porém não houve prova de que a ré, ao efetuar investigação acerca da autoria das irregularidades, tenha agido com abuso de direito. O poder de controle é um dos poderes conferidos pela lei ao empregador, que confere o direito de fiscalização do empregador sobre a atividade profissional do empregado, seja no exercício de suas funções, seja no ambiente interno da empresa, não podendo, esta, ultrapassar a dignidade do trabalhador ou demonstrar laços de discriminações entre os mesmos. No caso, não é possível verificar que a empresa tenha exercido seu poder de controle em excesso. Isso porque, pelo que foi possível constatar, a reclamada realizou suas investigações em caráter privado (em entrevistas individuais, consoante relatado pelo informante É.L.C.S. e confirmado pela testemunha F.B.C., que ainda aduziu que os depoimentos eram colhidos fora da filial em que os empregados laboravam), sem realizar acusações diretas (pois a única testemunha compromissada não relatou que algum empregado houvesse sido diretamente acusado), e sem uso de ‘detector de mentiras’ (conforme relatado pela testemunha inquirida). Ademais, não há elementos que permitam concluir que a ré foi a responsável pela divulgação da denúncia e da sindicância aos demais empregados da empresa” (TST, AIRR-2138-55.2010.5.04.0000, rel. Márcio Eurico Vitral Amaro, j. 1º-9-2010).

“*Justa causa. Falta grave.* Violação do art. 5º, XII e LIV, da CF. Divergência jurisprudencial. Pede a reforma do julgado que excluiu a resolução motivada do contrato de trabalho, ao argumento de que não houve violação à privacidade com o monitoramento, por meio de correio eletrônico, das conversas que o autor mantinha dentro de seu ambiente de trabalho. Transcreve o depoimento pessoal do autor e de várias testemunhas. Considerou a 2ª Turma do Regional que ao empregador é facultado monitorar e rastrear a atividade do empregado no ambiente de trabalho em *e-mail* corporativo, considerado ferramenta de trabalho, acrescentando que o *e-mail* pessoal ou particular do empregado definitiva da proteção constitucional e legal de inviolabilidade, sendo ilícitas as provas por ele obtidas. Consta do acórdão, à fl. 187: ‘(...) No entanto, a jurisprudência somente vem admitindo a possibilidade de o empregador monitorar

e rastrear a atividade do empregado no ambiente de trabalho, em *e-mail* corporativo. Ocorre que, no presente caso, os documentos das fls. 107/119 não foram extraídos do *e-mail* corporativo, pois trata-se de monitoramento de conversas de *e-mail* de uso pessoal. Saliento que o *e-mail* pessoal ou particular do empregado desfruta da proteção constitucional e legal de inviolabilidade, sendo ilícitas as provas por ele obtidas. Logo, mantenho do posicionamento adotado pelo Julgador de 1º grau de não conhecer das peças juntadas das fls. 107/119. Nessa linha, denoto que a própria natureza da questão, ou seja, a ocorrência ou não de motivo para a dispensa por justa causa, resolve-se primordialmente à mercê da apreciação dos subsídios documentais e testemunhais esgotados pelo Órgão Regional, que detém a última palavra na avaliação do conjunto probatório. Fica claro que o intento recursal é o revolvimento do conjunto fático-probante, o que não se coaduna com a natureza excepcional do recurso de revista, conforme a ilação autorizada pela Sumula n. 126 do TST, segundo a qual a discussão dos fatos e das provas finda nesta instância trabalhista. Ante o matiz absolutamente fático da controvérsia, resta prejudicada a pretendida violação a preceitos de lei e eventual análise de divergência pretoriana (fls. 96/96v)” (TST, AIRR 426540-10.2007.5.12.0036, rel. Min. João Batista Brito Pereira, j. 25-8-2010).

“*Correio eletrônico. Monitoramento. Legalidade.* Não fere norma constitucional a quebra de sigilo de *e-mail* corporativo, sobretudo quando o empregador dá a seus empregados ciência prévia das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. (...) Comungo do entendimento *a quo* no sentido de afastar a alegada ofensa aos incisos X, XII, LVI do art. 5º constitucional, por não ferir norma constitucional a quebra de sigilo de *e-mail* fornecido pela empresa, sobretudo quando o empregador avisa a seus empregados acerca das normas de utilização do sistema e da possibilidade de rastreamento e monitoramento de seu correio eletrônico. Também o julgado recorrido consignou ter o empregador o legítimo direito de regular o uso dos bens da empresa, nos moldes do art. 2º da CLT, que prevê os poderes diretivo, regulamentar, fiscalizatório e disciplinar do empregado, inexistindo notícia acerca de excessiva conduta derivada do poder empresarial” (TST, Ag. Instr. em RR 1130/2004-047-02-40, rel. Min. Vieira de Mello Filho, j. 31-10-2007).

3 — OFENSAS POR MEIOS ELETRÔNICOS

DIREITO À PRIVACIDADE x DEVER DE INFORMAÇÃO

Comentários:

Em razão da falsa aparência de anonimato e de ser a Internet uma “terra sem lei”, as ofensas propagadas por meios eletrônicos tornaram-se muito comuns no dia a dia. Lembramos que a Constituição Federal garante a liberdade de expressão, mas proíbe o anonimato, o que legitima a identificação do agente para posterior responsabilização.

Aos meios eletrônicos se aplicam as mesmas regras já aplicáveis aos delitos cometidos por outros meios, como, por exemplo, nos crimes contra a honra. Por isso, cresce a responsabilidade de quem publica manifestações de pensamento na Internet e também daqueles que viabilizam os meios para tanto.

“Apelação cível. Obrigação de fazer e não fazer. “Blog”. Veiculação virtual de conteúdo ofensivo por parte do responsável pelo “blog” e por terceiros. Tutela antecipada deferida para retirada do conteúdo ofensivo à honra e imagem do autor. Deferimento. Indeferimento da petição inicial por impossibilidade jurídica do pedido e extinção do processo sem resolução do mérito. Réu citado e que integrou a relação processual. Na fase recursal ofereceu contrarrazões ao recurso. Extinção afastada. Julgamento nos termos do art. 515, § 3º, do CPC. Responsabilidade pelo autor do blog em gerenciar o conteúdo da matéria postada. Desnecessidade de enviar o número dos IPs (Internet Protocol) dos correspondentes do referido blog. Recurso parcialmente procedente” (TJSP, Apelação n. 994.09.319036-5, rel. Des. Egidio Giacoia, j. 17-8-2010).

“Agravado de instrumento. Decisão de indeferimento de antecipação de tutela requerida a fim de que os réus se abstenham de utilizar a marca krav-magá e de fazer referência aos nomes dos autores e às suas atividades em publicações. Recurso dos autores. Verossimilhança das alegações autorais no sentido de que o segundo réu, através da Internet, faz comentários e alusões maldosos à pessoa dos 1º e 3º autores no sentido de desprestigiar-los e de questionar a legitimidade de suas atividades, o que poderá causar-lhes grave lesão ou dano de difícil reparação, com a ofensa à sua honra e à sua dignidade. Deferimento parcial da tutela antecipada, de natureza inibitória com fim de prevenção do ilícito, para que os réus se abstenham de fazer qualquer referência aos nomes e atividades dos autores

em qualquer contexto opinativo, e retirem de circulação qualquer publicação naquele sentido. Jurisprudência desta Corte. Manutenção da decisão agravada na parte em que indefere o pedido de abstenção do uso da marca *krav-magá* pelos réus, eis que a questão deve ser submetida ao contraditório, dependendo de maior instrução probatória. Recurso parcialmente provido” (TJRJ, Agravado de Instrumento 0065143-19.2009.8.19.0000, rel. Marco Aurélio Bezerra de Melo, j. 13-7-2010).

“Ação inibitória fundada em violação do direito à imagem, privacidade e intimidade de pessoas fotografadas e filmadas em posições amorosas em areia e mar espanhóis. Esfera íntima que goza de proteção absoluta, ainda que um dos personagens tenha alguma notoriedade, por não se tolerar invasão de intimidades (cenas de sexo) de artista ou apresentadora de TV. Inexistência de interesse público para se manter a ofensa aos direitos individuais fundamentais (arts. 1º, III, e 5º, V e X, da CF). Manutenção da tutela antecipada expedida no Agravado de Instrumento 472.738-4 e confirmada no julgamento do Agravado de Instrumento 488.184-4/3. Provimento para fazer cessar a divulgação dos filmes e fotografias em websites, por não ter ocorrido consentimento para a publicação. Interpretação dos arts. 461 do CPC, 12 e 21, do CC, preservada a multa diária de R\$ 250.000,00, para inibir transgressão ao comando de abstenção” (TJSP, Apelação cível 556.090.4/4-00, rel. Carlos Teixeira. L. Filho, j. 12-6-2008).

“Obrigação de fazer. Liminar. Pedido da autora para que a ré exclua dos seus bancos de dados todas as matérias veiculadas na Internet que contenham seu nome de fantasia. Indeferimento do pedido. Manutenção. Ausência dos requisitos legais. Autora que é pessoa jurídica atuante no ramo de consultoria em gestão empresarial, voltada à preparação e intermediação de candidatos a vagas no mercado de trabalho. Não se vê, a priori, prevalência do direito à honra e bom nome invocado pela autora sobre o direito de expressão e de informação dos ‘internautas’. Não pode a autora ofertar serviços na rede mundial de computadores, aproveitar as mensagens e conceitos favoráveis de clientes, mas pretender excluir as críticas dos consumidores descontentes. Interesse público na divulgação de críticas a serviços ofertados em relação de consumo no mundo digital. Recurso não provido” (TJSP, Agravado de Instrumento 566.550.4/2-00, rel. Francisco Loureiro, j. 24-4-2008).

“Constitucional. Dano moral. Art. 5º, V e X, da CF/88. Veiculação maliciosa de notícia em jornal e página da Internet. CRTR — 4ª Região. Sentença confirma-

da. I — Evidente a ofensa à honra e à imagem, merece a correta reprimenda judicial, através da fixação do dano moral e da retirada da informação da página mantida pelo Conselho-Réu na Internet, devendo a indenização por dano moral ser fixada em patamares razoáveis, de modo a aquilatar a ofensa efetivamente realizada, não podendo ser estabelecida em valor tão elevado que importe em enriquecimento sem causa, nem tão baixo que o ofensor esteja incentivado a reincidir em sua conduta. II — Reza o art. 5º, V, da *Lex Magna* que 'é assegurado o direito de resposta, proporcional do agravo, além de indenização por dano material, moral ou à imagem', dispondo, outrossim, seu inciso X, que 'são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação'. III — Não se verificando qualquer ilegalidade e não havendo provas que ratifiquem as matérias lançadas no jornal, irretocável a r. sentença ora atacada. IV — O direito à indenização surge quando a publicação transborda do simples objetivo de informação, atingindo a honra e a imagem dos indivíduos. V — Sentença mantida. VI — Remessa necessária e apelação a que se nega provimento" (TRF, 2ª Região, Apelação Cível 1999.51.01.000353-2, rel. Fernando Marques, publ. 28-10-2008).

"Reparação de danos. Ofensa à honra, moral e imagem. Fotografia de pessoa publicada em revista especializada e divulgada pela Internet em matéria jornalística sobre fraude em licitação de computadores de que o fotografado não participou. Vinculação da fotografia ao conteúdo da notícia. Comportamento negligente da empresa de comunicação. Indenização arbitrada com base no direito comum. Afastada a lei de imprensa. 1. Publicar em revista especializada e ainda divulgar pela Internet fotografia de pessoa que não tem nada a ver com a matéria jornalística que denuncia a ocorrência de fraude em licitação de computadores implica em violação do direito à privacidade e à imagem da pessoa, passível de indenização, mormente quando se constata que tal pessoa foi fotografada quando trabalhava com computadores e que a divulgação de sua imagem aos fatos denunciados, ocasionou-lhe chacotas e piadas de mau gosto e passou ela a ser chamada de corrupta. 2. A indenização do dano moral deve ser fixada de acordo com os parâmetros ditados pelo direito comum, visto que a tarifação prevista na lei de imprensa restou derogada com o advento da carta magna de 1988, não mais ficando o magistrado adstrito aos valores estabelecidos naquela lei para fixar o valor da indenização em razão de matérias ofensivas divulgadas pelos meios de comunicação. 3. O quantum indenizatório deve ser arbitrado em valor suficiente para produzir efeitos compensatórios, punitivos e preventivos. 4. Recurso da ré conhecido e parcialmente provido apenas para reduzir o valor da indenização a R\$

10.000,00 (dez mil reais)" (TJDF, 4ª Turma Cível, APC 20010510017570, rel. Roberval Casemiro Belinati, DJ 3-10-2006).

RESPONSABILIDADE DAS LAN HOUSES PELO CADASTRO DE SEUS USUÁRIOS

"Ação de obrigação de fazer cumulada com perdas e danos. Mensagem eletrônica recebida pela autora de teor ofensivo à sua honra. Obrigação do estabelecimento de onde partiu o envio de manter cadastro atualizado dos usuários, a fim de que estes não se favoreçam do anonimato quando da prática de ilícitos. Aplicação da Lei Estadual n. 12.228/2006, que obriga os estabelecimentos que fornecem serviços de acesso à Internet de manter referido cadastro. Atividade destes estabelecimentos que pode ser considerada de risco, caso não tomem as medidas necessárias que possibilitem a identificação dos usuários (art. 927, parágrafo único, do Código Civil). Responsabilidade civil pelos danos causados caracterizada. Cabimento do pedido alternativo para conversão em perdas e danos. Procedência mantida. Recurso desprovido" (TJSP, Apelação 604.346-4/7-00, rel. Des. Salles Rossi, j. 10-12-2008).

DELITOS CONTRA A HONRA NA INTERNET

"Ação de indenização. Dano moral. Orkut. Rede social. Sítio de relacionamento. Internet. Provedor de serviços de informações. Responsabilidade por fato do serviço. Direito do consumidor. Responsabilidade objetiva. Usuário vítima do evento. Ofensas de cunho moral. Expressão 'fazendo a fila andar'. Quantum. Os provedores de acesso são aqueles que possibilitam ao usuário o acesso à Internet e a armazenagem de conteúdo e aplicações que dão vida ao meio virtual. Os provedores de serviços ou informações alimentam a rede com dados (conteúdo e aplicações que tornam a própria Internet útil e interessante) que podem ser armazenados em provedores de acesso. A relação entre os provedores e usuários da Internet é regida pelas normas do Código de Defesa do Consumidor. Por consumidor conceitua-se 'toda pessoa física ou jurídica que adquire ou utiliza produtos ou serviços como destinatário final', abrangendo os usuários da Internet que se utilizam das redes sociais. Os provedores se enquadram como fornecedores de serviços descritos no art. 3º do CDC, visto que são pessoas jurídicas que desenvolvem as atividades

de criação, transformação, distribuição e comercialização de serviços de informação telemática a ser utilizada no meio virtual. A teor do art. 17 do CDC, quanto à responsabilidade por fato do serviço, equiparam-se aos consumidores todas as vítimas do evento, qual seja, a ofensa realizada por meio da rede social *Orkut*, não sendo sequer imprescindível que o ofendido seja usuário dos serviços do provedor de informações. A expressão 'fazendo a fila andar', aposta por usuário inidôneo na denominação do perfil pessoal da usuária, atinge a sua honra subjetiva. A expressão 'fazer a fila andar', no jargão popular, significa sucessão de parceiros amorosos, denotando promiscuidade por meio de relacionamento sexual não monogâmico, ou seja, com muitos parceiros diferentes. Fica ao arbítrio do magistrado a fixação do *pretium doloris*, devendo, contudo, ser observados parâmetros razoáveis para que seja atendido tanto o caráter punitivo da parte que deu causa, bem como o sofrimento psíquico e moral suportado pela vítima. Apelo parcialmente provido. V.V." (TJMG, Recurso 1.0145.08.471404-0/001(1), rel. Cabral da Silva, j. 3-8-2010).

"Dano moral. Publicação em blog na Internet e em jornal escrito. Excesso. Animus difamandi. Dever de indenizar. Fixação do quantum. Correção monetária. Juros moratórios. Termos iniciais. Sucumbência recíproca. Não verificação. 1. Configura-se o dever de indenizar, quando a notícia veiculada em *blog* na Internet e em jornal escrito não se limita à mera informação ou reprodução de fatos, acabando por ultrapassar os limites da liberdade de imprensa e atingir a honra da vítima, através do *animus difamandi*. 2. O arbitramento da indenização por danos morais deve se pautar nas condições pessoais e econômicas das partes envolvidas, no caráter reparatório e pedagógico da condenação, na extensão do dano sofrido, e também no princípio da proporcionalidade, que corresponde a uma moeda de duas faces: de um lado, proíbe-se o excesso; de outro, proíbe-se a proteção deficiente. 3. Fixados os danos morais na sentença, a correção monetária e os juros moratórios incidem a partir da data em que ela foi proferida. 4. O arbitramento do dano moral em valor inferior ao pleiteado na inicial não caracteriza sucumbência recíproca" (TJMG, Recurso 1.0145.07.424326-5/001(1), rel. Guilherme Luciano Baeta Nunes, j. 13-7-2010).

"Processual civil. Ação de obrigação de fazer cumulada com indenização por danos morais. Ofensas irrogadas à autora via Orkut. Relação de consumo. Responsabilidade objetiva da Google Brasil Internet Ltda., que não se escusa diante de fato de terceiro que, igualmente, integra a comunidade. Precedentes da corte e do colendo STJ. Damnum in re ipsa. Valor indenizatório que deve atender aos princípios da proporcionalidade, razoabilidade, sem se perder de vista o aspecto pedagógico da condenação.

Recurso provido ao abrigo do art. 557, § 1º-A, do Código de Processo Civil, de forma parcial. I — 'Para a caracterização da relação de consumo, o serviço pode ser prestado pelo fornecedor mediante remuneração obtida de forma indireta', proclama o colendo Superior Tribunal de Justiça, com ressonância em nossa Corte; II — Integrante da comunidade Orkut não é terceiro. Assim, indiscutível a responsabilidade da empresa Google Brasil Internet Ltda. pela violação à intimidade, à vida privada, à honra e à imagem dos seus membros, cabendo-lhe, se entender, promover ação de regresso em face do responsável pelo dano; III — "A Internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e infenso à responsabilidade pelos abusos que lá venham a ocorrer. No mundo real, como no virtual, o valor da dignidade da pessoa humana é um só, pois nem o meio em que os agressores transitam nem as ferramentas tecnológicas que utilizam conseguem transmutar ou enfraquecer a natureza de sobreprincípio irrenunciável, intransferível e imprescritível que lhe confere o Direito brasileiro. Quem viabiliza tecnicamente, quem se beneficia economicamente e, ativamente, estimula a criação de comunidades e páginas de relacionamento na Internet é tão responsável pelo controle de eventuais abusos e pela garantia dos direitos da personalidade de internautas e terceiros como os próprios internautas que geram e disseminam informações ofensivas aos valores mais mezinhos da vida em comunidade, seja ela real, seja virtual' (REsp 1117633/RO, rel. o respeitável Ministro Herman Benjamin); IV — O valor indenizatório, se por um lado deve atender aos princípios da proporcionalidade e da razoabilidade, por outro deve atentar para os aspectos pedagógicos da condenação, forma de, através do princípio da intimidação, evitarem-se práticas atentatórias à dignidade humana; V — Recurso provido ao abrigo do art. 557, § 1º-A, do Código de Processo Civil, de forma parcial" (TJRJ, Apelação 0013498-93.2007.8.19.0203, rel. Marco Ademir Pimentel, j. 7-7-2010).

"Indenização. Responsabilidade Civil. Danos Morais Inocorrência. Alegado controle do provedor sobre o conteúdo de vídeo ofensivo a imagem da empresa autora em sítio eletrônico por ele mantido ('Youtube'). Ausência de responsabilidade do provedor de serviços de Internet ('Google') pelas informações veiculadas. Inexistência de dever legal ou convencional de controle ou fiscalização prévia de conteúdo. Dados que foram publicados exclusivamente por terceiros. Nexo de causalidade inexistente entre a conduta lícita da Requerida e os danos não demonstrados. Sentença mantida. Recurso de apelação improvido" (TJSP, Apelação 990.10.209684-0, rel. Des. Vito Gugliemi, j. 27-6-2010).

“Apelação cível. Ação indenizatória. Dano moral. Ofensas através de site de relacionamento. Orkut. Responsabilidade civil objetiva. Aplicação obrigatória. Dever de indenizar. Reconhecimento. Quantum indenizatório. Fixação. Prudência e moderação. Observância necessária. I — Restando demonstrado nos autos que a apelante (Google Brasil) atua como representante da Google Inc., no Brasil, fazendo parte do conglomerado empresarial responsável pelo site de relacionamento denominado Orkut, compete-lhe diligenciar no sentido de evitar que mensagens anônimas e ofensivas sejam disponibilizadas ao acesso público, pois, abstendo-se de fazê-lo, responderá por eventuais danos à honra e dignidade dos usuários decorrentes da má utilização dos serviços disponibilizados. II — Aplica-se à espécie o art. 927, parágrafo único, do Código Civil, que adota a teoria da responsabilidade civil objetiva, estabelecendo que haverá obrigação de reparar o dano, independentemente de culpa, quando a atividade normalmente desenvolvida implicar, por sua natureza, risco para os direitos de outrem. III — No arbitramento do valor da indenização por dano moral devem ser levados em consideração a reprovabilidade da conduta ilícita e a gravidade do dano impingido, de acordo com os princípios da razoabilidade e proporcionalidade, cuidando-se para que ele não propicie o enriquecimento imotivado do recebedor, bem como não seja irrisório a ponto de se afastar do caráter pedagógico inerente à medida” (TJMG, Recurso 1.0024.08.061950-5/001(1), rel. Luciano Pinto, j. 17-7-2010).

“Agravado inominado. Responsabilidade civil. Provedor de internet. Dano moral. Ofensas à honra operadas através de comunidade do Orkut. Responsabilidade do Google por não ter retirado as páginas do ar após comunicação. 1 — O espólio tem legitimidade para pleitear o direito patrimonial à indenização pelos danos morais sofridos pelo de cujus em vida. 2 — Aplica-se aos provedores de conteúdo da Internet o disposto no Código de Defesa do Consumidor, por verificar-se a existência de remuneração indireta em sua atividade. 3 — Verifica-se defeito do produto quando o provedor, após comunicado da utilização de seu sítio para promover ofensas à dignidade alheia, não toma providências para removê-las. 4 — Indenização fixada em quatro mil reais, ponderando-se o alcance internacional das lesões com a gravidade do seu teor, em vista das condições pessoais da vítima. Agravado inominado a que se nega provimento” (TJRJ, Apelação 0380464-52.2008.8.19.0001, rel. Marcia Alvarenga, j. 26-5-2010).

“Dano moral. Injúria. Ofensa à honra. Advogado. Cuida de ação de reparação por danos morais em razão de alegada ofensa à honra. Aduz o autor que concedeu entrevista ao jornal Correio a respeito de fatos envolvendo o falecido artista Raul Seixas e os direitos deixados às três filhas e herdeiras, tendo sido a matéria

*veiculada no jornal e na ‘Internet’. Afirmo o autor, que a ré, ao ser ouvida pela jornalista para dar sua versão dos fatos, referiu-se a ele como ‘advogado idiota’, ofendendo-o. Na reportagem concedida, o autor se opôs às condutas da ré em relação à administração do patrimônio imaterial do artista, motivo pelo qual a ré foi consultada pela jornalista para dar sua versão em relação aos fatos. A ré é pessoa pública e, como tal, tem ciência das consequências trazidas por uma declaração ofensiva perpetrada contra outrem, por meio da imprensa. Poderia a ré refutar as afirmações prestadas pelo autor à jornalista, dar sua versão dos fatos, defender sua condição de companheira ou viúva do artista falecido, sem ultrapassar os limites da boa educação, injuriando o autor. O reconhecimento que o meio artístico, os amigos e fãs do artista têm em relação à ré não se confunde com o contorno jurídico da questão, de modo que era autorizado ao autor, como advogado, expor a situação fática ao jornal e externar sua opinião jurídica. A afirmação da ré colocou o autor em situação vexatória, sendo patente seu ânimo de atingir a honra do autor. Deflagra-se, portanto, a reparação dos danos morais perpetrados ao autor, recaiando a responsabilização civil sobre a ré com fulcro nos arts. 186 e 927, II, ambos do Código Civil. Com efeito, a reparação dos danos morais ancora-se em três princípios: *neminem laedere*; *restitutio in integro* e *id quod interest* — restaurar o interesse violado quando possível, atendendo às funções: a) punitiva desestímulo (“punitive damage”); b) pedagógica; e c) compensatória — dor, sofrimento perpetrados à vítima, *in re ipsa*. Diante de tais premissas, das circunstâncias fáticas do caso concreto, bem como a capacidade econômica da ré, fixa-se o *quantum* reparatório em R\$ 5.000,00. Provimento do recurso”* (TJRJ, Apelação 0109103-22.2009.8.19.0001, rel. Roberto de Abreu e Silva, j. 25-5-2010).

“Processual penal. Conflito negativo de competência. Notícia-crime pela suposta prática dos delitos previstos nos arts. 20 e 21 da Lei n. 5.250/97 (Lei de Imprensa). Lei não recepcionada pela Constituição Federal. ADPF 130/DF. Aplicação dos arts. 138 e 139 do CP e art. 70 do CPP. Duas sequências de fatos distintos. Publicação de reportagens veiculadas na revista IstoÉ. Competência do juízo do local da impressão da revista. Matérias disponibilizadas no blog ‘conversa afiada’. Competência do local em que praticados os atos de publicação. Conflito conhecido. Competência da Justiça Federal paulista. 1. Não recepcionada a Lei de Imprensa pela nova ordem Constitucional (ADPF 130/DF), quanto aos crimes contra a honra, aplicam-se, em princípio, as normas da legislação comum, quais sejam, arts. 138 e seguintes do Código Penal e arts. 69 e seguintes do Código de Processo Penal. 2. Na hipótese de crime contra a honra praticado por meio de publicação impressa de periódico, deve-se fixar a competência do Juízo onde ocorreu a impressão, tendo em vista ser o primeiro local onde as matérias produzidas chegaram ao conhecimen-

to de outrem, nos moldes do art. 70 do Código de Processo Penal. Remanesce, na prática, o resultado processual obtido pela antiga aplicação da regra de competência prevista na não recepcionada Lei de Imprensa. 3. Crimes contra a honra praticados por meio de reportagens veiculadas pela Internet ensejam a competência do Juízo do local onde foi concluída a ação delituosa, ou seja, onde se encontrava o responsável pela veiculação e divulgação de tais notícias. 4. Conhecimento do conflito para declarar competente o Juízo Federal da 4ª Vara Criminal da Seção Judiciária do Estado de São Paulo” (STJ, CC 106.625/DF, rel. Min. Arnaldo Esteves Lima, j. 12-5-2010).

“Processual civil. Orkut. Ação civil pública. Bloqueio de comunidades. Omissão. Não ocorrência. Internet e dignidade da pessoa humana. Astreintes. Art. 461, §§ 1º e 6º, do CPC. Inexistência de ofensa. 1. Hipótese em que se discutem danos causados por ofensas veiculadas no Orkut, ambiente virtual em que os usuários criam páginas de relacionamento na Internet (= comunidades) e apõem (= postam) opiniões, notícias, fotos etc. O Ministério Público Estadual propôs Ação Civil Pública em defesa de menores — uma delas vítima de crime sexual — que estariam sendo ofendidas em algumas dessas comunidades. 2. Concedida a tutela antecipada pelo Juiz, a empresa cumpriu as determinações judiciais (exclusão de páginas, identificação de responsáveis), exceto a ordem para impedir que surjam comunidades com teor semelhante. 3. O Tribunal de Justiça de Rondônia reiterou a antecipação de tutela e, considerando que novas páginas e comunidades estavam sendo geradas, com mensagens ofensivas às mesmas crianças e adolescentes, determinou que o Google Brasil as impedisse, sob pena de multa diária de R\$ 5 mil, limitada a R\$ 500 mil. 4. Inexiste ofensa ao art. 535 do CPC. No mérito, o Google impugna a fixação das astreintes, suscitando ofensa ao art. 461, §§ 1º e 6º, do CPC ao argumento de sua ineficácia, pois seria inviável, técnica e humanamente, impedir de maneira prévia a criação de novas comunidades de mesma natureza. No mais, alega que vem cumprindo as determinações de excluir as páginas indicadas pelo MPE e identificar os responsáveis. 5. A Internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e inenfoque à responsabilidade pelos abusos que lá venham a ocorrer. 6. No mundo real, como no virtual, o valor da dignidade da pessoa humana é um só, pois nem o meio em que os agressores transitam nem as ferramentas tecnológicas que utilizam conseguem transmutar ou enfraquecer a natureza de sobreprincípio irrenunciável, intransferível e imprescritível que lhe confere o Direito brasileiro. 7. Quem viabiliza tecnicamente, quem se beneficia economicamente e, ativamente, estimula a criação de comunidades e páginas de relacionamento

na Internet é tão responsável pelo controle de eventuais abusos e pela garantia dos direitos da personalidade de internautas e terceiros como os próprios internautas que geram e disseminam informações ofensivas aos valores mais cotidianos da vida em comunidade, seja ela real, seja virtual. 8. Essa corresponsabilidade — parte do compromisso social da empresa moderna com a sociedade, sob o manto da excelência dos serviços que presta e da merecida admiração que conta em todo mundo — é aceita pelo Google, tanto que atuou, de forma decisiva, no sentido de excluir páginas e identificar os gangsters virtuais. Tais medidas, por óbvio, são insuficientes, já que reprimir certas páginas ofensivas já criadas, mas nada fazer para impedir o surgimento de outras tantas, com conteúdo igual ou assemelhado, é, em tese, estimular um jogo de Tom e Jerry, que em nada remedia, mas só prolonga, a situação de exposição, de angústia e de impotência das vítimas das ofensas. 9. O Tribunal de Justiça de Rondônia não decidiu conclusivamente a respeito da possibilidade técnica desse controle eficaz de novas páginas e comunidades. Apenas entendeu que, em princípio, não houve comprovação da inviabilidade de a empresa impedi-las, razão pela qual fixou as astreintes. E, como indicado pelo Tribunal, o ônus da prova cabe à empresa, seja como depositária de conhecimento especializado sobre a tecnologia que emprega, seja como detentora e beneficiária de segredos industriais aos quais não têm acesso vítimas e Ministério Público. 10. Nesse sentido, o Tribunal deixou claro que a empresa terá oportunidade de produzir as provas que entender convenientes perante o juiz de primeira instância, inclusive no que se refere à impossibilidade de impedir a criação de novas comunidades similares às já bloqueadas. 11. Recurso Especial não provido” (STJ, REsp 1.117.633/RO, rel. Ministro Herman Benjamin, j. 9-3-2010).

“Apelação cível. Responsabilidade civil. Perfil falso criado no site de relacionamentos Orkut. Inserção de características pejorativas. Agressão à honra. Dano moral configurado. Responsabilidade do provedor de hospedagem por omissão. Denúncia de abuso não atendida tempestivamente. É certo que o provedor de hospedagem se limita a disponibilizar espaço para armazenamento do endereço na Internet, ordinariamente não respondendo pelo conteúdo do site armazenado. Contudo, em ocorrendo a prática de ato ilícito pelo autor do site, é dever do hospedeiro, se assim for instado pelo interessado, pela vítima, o de retirar imediatamente da rede o referido site. Sua omissão, sem relevante razão de direito, configura agir culposos e colore a figura do ato ilícito, fazendo com que responda pelos danos que a manutenção do site na rede venha a causar ao prejudicado. Responsabilidade civil subjetiva do provedor de hospedagem configurada diante da inércia em atender ao pedido da vítima, o que somente ocorreu após o aforamento da ação, com o deferimento de medida liminar

que determinou o cancelamento do perfil falso no Orkut, e sob pena de multa, *Apelação provida*” (Segredo de Justiça) (TJRS, *Apelação cível* 70033563297, rel. Paulo Antônio Kretzmann, j. 25-3-2010).

“Apelação cível. Responsabilidade civil. Dano moral. Orkut. Criação de perfil falso. Responsabilidade civil objetiva. Caso concreto. Ação de indenização por danos morais proposta em desfavor da Google, empresa proprietária de mecanismo de busca de assuntos na Internet, que provê também o Orkut, serviço de hospedagem de páginas e informações. O autor criou uma página pessoal — perfil — no Orkut; no entanto, um terceiro não identificado criou um perfil falso, usando duas fotografias pessoais do autor, redigindo frases apelativas e filiando-se a comunidades com ‘gostos esdrúxulos’. Tal perfil falso teve o acesso de amigos e colegas de trabalho. Responsabilidade civil objetiva. É razoável, para evitar discriminações, a política do site, no sentido de remover apenas mediante ordem judicial perfis que contenham imagem ou linguagem chocante ou repulsiva e sátira política ou social. Porém, tratando-se de atividade de risco — com a qual a ré auferiu lucro, destaque-se —, em que qualquer pessoa pode facilmente criar falsos perfis, causando, assim, dano à honra e imagem de outrem, é caso de responsabilidade civil objetiva, nos termos do art. 927, parágrafo único, do CPC. Ou seja, se este risco é inevitável e a ré o assume, diante dos benefícios que obtém, responde pelos prejuízos. Mesmo não sendo a ré responsável pela elaboração do perfil falso e mesmo sendo o conteúdo deste inserido entre as matérias que, segundo seu estatuto, a demandada se propôs a excluir apenas mediante ordem judicial, se a parte prejudicada tomou as providências necessárias a seu alcance para evitar o dano — no caso, acionou a ferramenta “denunciar abusos” —, configura-se o dever de indenizar. Apelo provido. Unânime” (TJRS, *Apelação Cível* 70034086116, rel. Iris Helena Medeiros Nogueira, j. 10-3-2010).

“Reparação de danos. Internet. Vinculação de página no site de relacionamentos Orkut a comunidade ofensiva. Montagem e disponibilização de foto da autora. Ofensa à honra da autora. Dano moral in re ipsa. Dever de indenizar. Quantum indenizatório mantido. Sentença confirmada por seus próprios fundamentos. 1. Terceiro não identificado apropriou-se da senha do ‘perfil’ da autora na rede de relacionamentos Orkut. A aludida página serviu para proferir ofensas à dignidade da autora, causando-lhe danos, os quais devem ser indenizados. 2. Tendo a empresa ré hospedado a página ofensiva, não providenciando sua exclusão mesmo após diversas solicitações feitas pela própria autora através do site, é aquela responsável pelos danos ocasionados à demandante, ainda que o ‘perfil’ falso tenha sido con-

feccionado por terceira pessoa. 3. A verba indenizatória arbitrada pelo juízo singular (R\$ 6.000,00) mostra-se proporcional à ofensa sofrida, pois, ainda que a comunidade ofensiva tenha permanecido disponível por sete dias apenas, houve divulgação da mesma para várias pessoas do relacionamento da autora, como se pode verificar pelos documentos de fls. 131 a 148. Imperioso, assim, a manutenção do valor da indenização fixada. Sentença mantida por seus próprios fundamentos. Recurso improvido” (TJRS, *Recurso Cível* 71002090603, rel. Saldanha da Fonseca, j. 17-9-2009).

“Indenização. Dano moral. Orkut. O prestador do serviço Orkut responde de forma objetiva pela criação de página ofensiva à honra e imagem da pessoa, porquanto abrangido pela doutrina do risco criado; decerto que, identificado o autor da obra maligna, contra ele pode se voltar, para reaver o que despendeu” (TJMG, *Recurso Cível* 1.0701.08.221685-7/001(1), rel. Ricardo Torres Hermann, j. 5-8-2009).

“Apelação cível. Responsabilidade civil. Indenização por danos morais. Comunidade falsa criada por terceiro em site de relacionamentos. Orkut. Ofensa à honra da autora. Ação dirigida contra o provedor, que hospeda a página da comunidade na Internet. Hosting service providers. Responsabilidade subjetiva. provedor de hospedagem que não está obrigado a fiscalizar, nem realizar qualquer censura prévia sobre o conteúdo inserido pelos usuários. Imprescindibilidade de se demonstrar a omissão ou recusa, do provedor, em não fazer cessar a ofensa, quando solicitado para tanto. Culpa não evidenciada nos autos. Responsabilidade exclusiva do autor da ofensa. Recurso conhecido a que nega provimento. 1. ‘O provedor de hospedagem não responde pelo conteúdo das informações armazenadas, exceto quanto à eventual responsabilidade subjetiva decorrente de negligência pela não solicitude quando da retirada dessas informações de suas páginas” (TJPR, 10ª Câmara Cível, *Apelação Cível* 0556020-1, rel. Des. Nilson Mizuta, j. 4-6-2009).

“(…) Segundo a denúncia, no dia 11 de junho de 2007, às 14:24 min., pela Internet, enviou a denunciada mensagem eletrônica (e-mail), para todos os computadores que formam a rede do Correio MPDFT, utilizada por todos os 344 (trezentos e quarenta e quatro) membros em atividade do Ministério Público do DF, intitulada ‘Como Age Nosso Corregedor’, com o propósito de atingir a honra subjetiva (...). ‘Penal e processual penal — Crimes contra a honra — Membros do Ministério Público. 1. Ao examinar-se a tipicidade dos delitos de difamação e injúria, é importante examinar o tempo e lugar de ocorrência dos fatos e as pecu-

liaridades da situação de cada denunciado. 2. No teatro de disputas políticas e de espaço de poder institucional, as condutas dos envolvidos nos fatos desencadeadores da denúncia criminal tornam desculpáveis possíveis ofensas, acusações e adjetivações indesejáveis. 3. Na avaliação contextual dos fatos pertinentes, não se identifica a vontade deliberada de difamar ou injuriar. 4. As ásperas palavras dirigidas à vítima, pela denunciada, soam como indignação pelos episódios institucionais vivenciados. 5. O crime de calúnia exige imputação de crime praticado pela vítima, por fato ou fatos determinados, o que incorreu na espécie. 6. Denúncia rejeitada” (STJ, Corte Especial, APn 516/DF, rel. Ministra Eliana Calmon, j. 20-8-2008).

“*Penal. Recurso especial. Calúnia. Ofensa veiculada na Internet. Exigência de publicidade da retratação, que deve ser cabal. Recurso especial improvido.* 1. Nos termos do art. 143 do Código Penal, a retratação, para gerar a extinção da punibilidade do agente, deve ser cabal, ou seja, completa, inequívoca. 2. No caso, em que a ofensa foi praticada mediante texto veiculado na Internet, o que potencializa o dano à honra do ofendido, a exigência de publicidade da retratação revela-se necessária para que esta cumpra a sua finalidade e alcance o efeito previsto na lei. 3. Recurso especial improvido” (STJ, REsp 320.958/RN, rel. Ministro Arnaldo Esteves Lima, j. 6-9-2007).

“*Diante do exposto*, por considerar que não mais subsistem os fundamentos para a manutenção da prisão preventiva, *concedo a liberdade provisória* aos acusados P.H.C.V., R.B.A.J. e R.T.S.O., impondo, porém, *a cada um dos réus*, o compromisso de cumprimento das seguintes condições: a) acompanhar todos os atos processuais e atender aos chamamentos judiciais; b) não se ausentar da comarca onde reside por mais de 24 (vinte e quatro) horas, sem prévia autorização deste Juízo; c) recolher-se à sua residência no horário máximo das 20:00h, ficando proibido de se ausentar de sua residência nos finais de semana e feriados; d) ocupar-se lícitamente; e) não frequentar locais suspeitos, tais como casas de prostituição e de tavolagem; f) comparecer quinzenalmente em Juízo, na 1ª (primeira) e na 3ª (terceira) semana de cada mês, para informar e justificar suas atividades, ressaltando que o acusado residente em outro Estado da Federação (P.H.C.V.) deverá comparecer no Juízo Federal com jurisdição em matéria penal sobre a cidade onde reside; g) não frequentar ‘lan houses’; h) não manter cadastro ou tela na rede de relacionamento ‘Orkut’ ou similar; i) não frequentar salas de ‘bate-papo’ virtual ou de MSN e semelhantes; j) matricular-se e frequentar imediatamente instituição de ensino que dê continuidade ao seu grau regular de estudo, comprovando em Juízo, trimestralmente, a assiduidade e aproveitamento em tal curso; l) não fazer uso de substâncias entorpecentes, inclusive o álcool; e m) realizar a leitura de obras literárias a serem

indicadas trimestralmente por este Juízo, devendo cada réu apresentar relatório, produzido de próprio punho, com o mínimo de 10 (dez) laudas, revelando suas impressões sobre os temas principais de cada livro, iniciando-se pelas obras (a) ‘A hora e a vez de Augusto Matraga’, último conto do livro ‘Sagarana’, do escritor Guimarães Rosa, e (b) ‘Vidas Secas’, de Graciliano Ramos, trabalhos literários que se encontram disponíveis em bibliotecas públicas desta cidade de Natal/RN. Determino, especificamente ao réu R.T.S.O., que se submeta a tratamento de desintoxicação contra o uso de drogas, a ser indicado por este Juízo em 10 (dias) dias, e que apresente trimestralmente relatório de aproveitamento terapêutico subscrito pelo profissional responsável. Alerta-se que a violação de quaisquer das obrigações e limitações ora impostas aos acusados recrudescerá o risco ponderável de repetição dos atos ilícitos que lhes são imputados, o que poderá acarretar a reconsideração da liberdade provisória. Expeça-se o Alvará de Soltura em favor de P.H.C.V., R.B.A.J. e R.T.S.O., se por motivo outro não devam permanecer presos. Determino aos réus o comparecimento a esta Segunda Vara Federal, no dia 17 de abril de 2008, às 17:00h, para audiência de advertência das condições” (STJ, HC 81.638, rel. Gilson Dipp, j. 12-6-2007).

RESPONSABILIDADE DOS SITES DE BUSCA

“(…) Assim, eventuais abusos ou ilicitudes em veiculações na Internet deverão ser informadas nos autos pelo autor agravado, com indicação da respectiva URL e, após análise de seu conteúdo, o d. Magistrado poderá determinar sua eventual remoção tanto dos sites buscadores como da própria página primária, desde que hospedada em domínios de responsabilidade de algum dos réus (...) Ementa: Agravado de instrumento. Obrigação de fazer. Tutela antecipada deferida para retirada do mundo virtual de endereços eletrônicos primários que estavam denegando a imagem do autor. Ampliação do alcance da medida para englobar outras URLs que surgiram no decorrer da demanda, com determinação também para eliminação desses sites dos resultados obtidos através dos buscadores mantidos pelos réus. Possibilidade. Determinação que não é genérica e não implica em exclusão por completo das páginas primárias, exceto quando os ditos endereços eletrônicos estiverem diretamente vinculados aos réus. Multa diária que se mostra bastante excessiva. Redução determinada. Recurso Parcialmente Provido” (TJSP, Agravo de Instrumento 990.10.110525-0, rel. Des. Egidio Giacoia, j. 3-8-2010).

“*Indenização.* Pedido para determinar a desativação da veiculação do nome do autor em processo criminal no site mantido pela agravante. Acesso de pesquisa disponível em site de Tribunal. Informações lançadas na Internet por terceiros.

Empresa-ré que apenas administra *site* que contém ferramenta de busca” (TJSP, Agravo de Instrumento 994.09.324863-1 (667.274-4/9-00), rel. Des. Silverio Ribeiro, j. 19-5-2010).

“Agravo de instrumento. Ação de obrigação de fazer com pedido de indenização. Antecipação de tutela. Provedor de serviços de busca na Internet (Google Search). Proibição da publicação de endereços de páginas eletrônicas que fazem alusão aos agravantes. Não cabimento. Páginas que meramente apresentam os endereços e não o conteúdo. Monitoramento prévio. Notória inviabilidade. Bloqueio que deve se limitar aos textos contidos em páginas hospedadas em domínios de titularidade da agravante. Recurso conhecido e parcialmente provido” (TJSC, Agravo de Instrumento 2009.047162-2, rel. Vilmar Cardozo, j. 6-4-2010).

“*Indenização por danos morais*. Internet. Divulgação de matéria ofensiva à honra do autor em *sites* da Internet. Requerida que apenas permite o acesso dos usuários mediante a ferramenta de busca que disponibiliza na rede, não podendo ser responsável pelo conteúdo das notícias ali veiculadas. Responsabilidade que deve ser atribuída ao criador do endereço eletrônico. Ademais, nada impede que qualquer usuário acesse diretamente o *site* sem a utilização do serviço de busca oferecido pela requerida, sendo inócua a liminar concedida. Requerida que notificada extrajudicialmente procedeu à exclusão dos *links* que divulgavam a notícia naquele momento. Ausência de descumprimento da ordem liminar ou de omissão. Improcedência mantida. Recurso improvido” (TJSP, Apelação 533.118.4/5-00, rel. Des. Salles Rossi, j. 27-3-2008).

4 — VAZAMENTO DE INFORMAÇÕES

SIGILO DE DADOS

Comentários:

A informação e o conhecimento formam parte do patrimônio intangível da empresa. Na sociedade atual, essas são a maior riqueza corporativa.

Assim, o empregador deve conscientizar os colaboradores sobre segurança da informação e monitorar a manipulação dos dados pelos mesmos, devendo ter cuidado, controle, classificar e restringir o acesso às informações sensíveis.

Na era digital, o vazamento de informações é cada vez mais comum, dada a facilidade de transmissão dos dados sigilosos pelos meios eletrônicos. Um simples *pen-drive* ou mesmo um MP3 pode representar uma enorme ameaça, caso utilizado de forma inadequada. Mas o monitoramento, para não ter risco legal, precisa ser avisado previamente, bem como sua aplicação tem que ser uniforme para todos, evitando, assim, qualquer alegação de arbitrariedade ou perseguição.

“*Ação de obrigação de fazer*. Identificação do titular da conexão da Internet para uso do IP. O direito ao sigilo dos dados cadastrais e de conexão referentes aos usuários da Internet não tem caráter absoluto. Inexistência da quebra de sigilo, mas tão somente fornecimento das informações cadastrais daquele que se serviu da Internet para obter ou conseguir objetivos considerados ilícitos. Ação procedente. Recurso improvido” (TJSP, Apelação 7.290.306-5, rel. Des. Carlos Alberto Lopes, j. 3-11-2008).

“I. Decisão judicial (...). II. Quebra de sigilo bancário: prejudicadas as alegações referentes ao decreto que a determinou, dado que a sentença e o acórdão não se referiram a qualquer prova resultante da quebra do sigilo bancário, tanto mais que, dado o deferimento parcial de mandado de segurança, houve a devolução da documentação respectiva. III. Decreto de busca e apreensão: validade. 1. Decreto específico, que somente permitiu que as autoridades encarregadas da diligência selecionassem objetos, dentre aqueles especificados na decisão e na sede das duas empresas nela indicadas, e que fossem ‘interessantes à investigação’ que, no caso, tinha pertinência com a prática do crime pelo qual foi efetivamente condenado o recorrente. 2. Ademais não se demonstrou que as instâncias de mérito tenham invocado prova não contida no objeto da medida judicial, nem tenham valorado qualquer dado resultante da extensão dos efeitos da decisão determinante da busca e apreensão, para que a Receita Federal e a ‘Fiscalização do INSS’ também tivessem acesso aos documentos apreendidos, para fins de investigação e cooperação

na persecução criminal, 'observado o sigilo imposto ao feito'. IV. Proteção constitucional ao sigilo das comunicações de dados — art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada — o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa — este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. A proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira — RTJ 179/225, 270). V. Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º, e 114, II; e Súmula 497 do Supremo Tribunal)" (STF, Tribunal Pleno, RE 418.416, rel. Min. Sepúlveda Pertence, DJ 19-12-2006).

"Agravado de instrumento. (...) Necessidade de fornecimento dos dados cadastrais daquele que veiculou as mensagens. Possibilidade técnica da recorrente em fornecer os dados. Legitimidade passiva reconhecida. Alegação de versibilidade da liminar. Afastamento. Inexistência de prejuízo irreparável. Violação de sigilo. Inocorrência. Fornecimento apenas dos dados cadastrais e não do conteúdo das mensagens. Multa diária. Cabimento. Decisão mantida. Agravado improvido" (TJSP, Agravado de Instrumento 558.467-4, rel. Eduardo Sadão Yonamine, j. 13-5-2008).

VAZAMENTO DE DADOS SIGILOSOS DA EMPRESA

"A duas, os meios modernos de comunicação, fax, e-mails e outros, usados de forma errada podem ocasionar graves danos. E têm a qualidade de rápida propagação da comunicação. Diversas listas de Internet já foram processadas, até mesmo pelo Ministério Público, tendo-se em consideração ofensas ou proselitismo criminoso. O direito à privacidade e ao sigilo não pode ser exercido contra a sociedade.

Ou por uns indivíduos contra outros. Até porque a Internet é pública e permite vazamento, provocado ou ocasional, de seu conteúdo. Não se pode afirmar taxativamente que exista segurança absoluta de sigilo nesse moderno e eficiente meio de comunicação. Ademais é cediço na doutrina e na jurisprudência que o empregador pode vigiar, impedir e punir as atitudes inconvenientes, como ofensas, sites pornográficos, ameaças etc., provenientes do uso indevido dos computadores por seus empregados. E se confere esse direito de vigiar porque que existe o conflito de dois interesses. O individual e o coletivo. E entendo que nesses casos o coletivo tem de ser privilegiado. (...) 'O caso em espécie é de descoberta acidental pelo empregador que a Autora cometera falta gravíssima, contrariando expresso dispositivo do contrato de trabalho, avençado por escrito, e repassava segredos comerciais da Reclamada para empresa concorrente. (...) Como assistente de importação e exportação detinha conhecimentos de segredos estratégicos e táticos da empresa. E tinha compromisso expresso de sigilo. E de tanto não se preocupou ao ceder, sem permissão, os dados que dispunha em razão do cargo ocupado. (...) Com os fundamentos supra dou provimento ao apelo da Reclamada para considerar justa a demissão tendo em vista a gravidade da falta cometida. (...)'" (TST, Ag. Instr. em RR 2771/2003-262-02-40, rel. Min. Maria de Assis Calsing, j. 2-4-2008).

"*Transação comercial. Site especializado da Internet. Prestação de serviço. Fraude. Captura de informações pessoais do cadastro.* (...) Nos casos de realização de transação comercial através de site especializado, responde a respectiva empresa pelas fraudes sofridas pelos seus clientes (...). Havendo o cadastramento do endereço eletrônico do cliente em seu banco de dados, através do qual se daria o contato com os possíveis compradores, configura defeito do serviço, se essa informação (...) ao conhecimento de estelionatário, que dela se utilizou para ludibriar a consumidora e obter o recebimento indevido da mercadoria anunciada. (...) Mas no caso presente, ela também estaria presente por força da violação do dever de preservação de informação restrita ou sigilosa" (TJDF, Recurso Inominado 20060110966598, rel. Luis G. B. de Oliveira, j. 18-3-2008).

"*Seguradora. Entrega de HD do computador. Dano moral configurado. Falta de dever de cuidado ao vender o bem sem apagar as informações pessoais do segurado.* Tendo a seguradora não diligenciado de forma correta ao efetuar a venda do HD sinistrado entregue pelo autor para o recebimento da indenização, sem apagar seus dados pessoais, expondo sua privacidade perante terceiros, faz jus à indenização extrapatrimonial. Recurso do autor parcialmente provido para majorar o valor da indenização. Recurso do réu desprovido e provido em parte o recurso do autor. Unânime" (TJRS, Recurso cível 71001199744, rel. João Pedro Cavalli Junior, j. 26-4-2007).

“Administrativo. Servidor público. Concurso público para perito criminal. Exame psicométrico. Candidato considerado inapto. Divulgação do conteúdo dos exames em fóruns de discussão da Internet. Vazamento de informações. Ofensa ao princípio constitucional da isonomia. Comprometimento da lisura do certame. Sentença mantida. Recurso não provido. Sentença mantida em sede de reexame necessário” (PR 0591090-5, 4ª Câmara Cível, rel. Salvatore Antonio Astuti, j. 2-3-2010).

VIOLAÇÃO DE DIREITOS AUTORAIS E DE IMAGEM

Comentários:

A Internet facilita o acesso e a disponibilização de conteúdos e, ao contrário do que possa parecer, o que está na rede mundial de computadores não é necessariamente de domínio público, motivo pelo qual deve-se ter atenção redobrada quando da utilização de conteúdo de terceiro, sob pena de violação de direitos autorais. O mesmo se aplica ao uso de imagem sem a devida autorização de seu titular e/ou retratado.

A evolução tecnológica desafia não apenas o Direito, mas a ética dos usuários. Assim como aprendemos o valor “não pegue o que não é seu”, agora aplicamos “não copie e cole o conteúdo do próximo”.

No caso de direito de imagem ainda é mais restritivo. Por isso deve-se ter muito cuidado ao coletar e usar imagem de pessoas obtidas na Internet. Às vezes, a foto tem a cessão de direitos autorais (*creative commons*), mas isso não quer dizer que há a cessão do direito de imagem da pessoa fotografada. E quem faz uso do conteúdo responde. Por isso, devemos buscar fontes seguras, legítimas e sempre citar a fonte e a autoria, com data e endereço do *link* de onde foi retirado.

“Responsabilidade civil. Ação de indenização por danos morais. Cerceamento de defesa inocorrente. Desnecessidade da produção de prova. Veiculação de filmagens reportagem em telejornais e “sites” da internet onde aparece imagem do autor sem que o mesmo tenha dado autorização. A prova a ser produzida nos autos tem a finalidade de formar a convicção do julgador. Se este entender que a prova constante nos autos é suficiente à formação da sua convicção, pode o mesmo passar de imediato ao julgamento do feito. Descabe ação de indenização por danos morais quando a filmagem e a reportagem veiculadas em telejornal e “sites” das empresas demandadas limitava-se a noticiar tão somente o fato (consumo e tráfico de drogas nas imediações da Delegacia de Polícia onde o autor prestava serviços de plantão), ausente caráter ofensivo ao autor. Atuação dentro das prerrogativas constitucionais do meio de comunicação ao noticiar fatos públicos com narração fidedigna e imparcial. Preliminar rejeitada. Mérito do recurso desprovido. Sentença mantida. Decisão unânime” (TJRS, Apelação Cível 70030092829, rel. Jorge Alberto Schreiner Pestana, j. 12-8-2010).

“Apelação cível. Cautelar produção antecipada provas. Assistência judiciária deferida grau recurso. Conhecimento. Sentença de procedência. Inconsistência. Homologação provas produzidas. Condenação honorários. Descabimento. Exclusão ônus sucumbência. Indenização por danos morais. Publicação site Internet. Fotos íntimas. Término relacionamento amoroso. Exposição vida íntima sexual do casal. Ausência de prova da autoria da página. Responsabilidade objetiva. Provedor. Teoria do risco. Relação de consumo configurada. Aplicação do código de defesa do consumidor. Indenização devida. Recursos conhecidos e parcialmente providos. Na ação cautelar de produção antecipada de provas cumpre ao magistrado a prolação de sentença meramente homologatória das provas produzidas, sendo incabível a condenação em sucumbência. Evidenciada a lesão ao direito e a responsabilidade pela indenização, no que concerne a exposição em espaço disponibilizado por provedor de Internet, que permite que qualquer pessoa utilize das ferramentas ali existentes para criação de página em que é veiculado conteúdo difamatório à honra dos usuários. Incumbe ao provedor filtrar as informações ali divulgadas, a fim de se evitar a propagação de crimes” (TJSC, Apelação Cível 2008.002917-6, rel. Marcelo Volpato de Souza, j. 28-7-2010).

“Apelação. Responsabilidade civil. Internet. Uso de imagem para fim depreciativo. Criação de flog — página pessoal para fotos na rede mundial de computadores. Responsabilidade dos genitores. Pátrio poder. Bullying. Ato ilícito. Dano moral in re ipsa. Ofensas aos chamados direitos de personalidade. Manutenção da indenização. Provedor de Internet. Serviço disponibilizado. Comprovação de zelo. Ausência de responsabilidade pelo conteúdo. Ação. Retirada da página em tempo hábil. Preliminar afastada. Denúnciação da lide. Ausência de elementos. Apelo do autor da denúnciação da lide. I. Para restar configurada a denúnciação da lide, nos moldes do art. 70 do CPC, necessários elementos demonstrando vínculo de admissibilidade. Ausentes provas embasando o pedido realizado, não há falar em denúnciação da lide. Da responsabilidade do provedor de Internet. II. Provedores de Internet disponibilizam espaço para criação de páginas pessoais na rede mundial de computadores, as quais são utilizadas livremente pelos usuários. Contudo, havendo denúncia de conteúdo impróprio e/ou ofensivo à dignidade da pessoa humana, incumbe ao prestador de serviços averiguar e retirar com brevidade a página se presente elementos de caráter ofensivo. III. Hipótese em que o provedor excluiu a página denunciada do ar depois de transcorrida semana, uma vez ser analisado assunto exposto, bem como necessário certo tempo para o rastreamento da origem das ofensas pessoais — PC do ofensor. Ausentes provas de desrespeito aos direitos previstos pelo CDC, não há falar em responsabilidade civil do provedor. Apelo da ré. Do dano moral. IV. A Doutrina moderna evoluiu para firmar entendimento acerca da responsabilidade civil do ofensor em relação ao ofendido, haja vista desgaste do instituto proveniente da massificação das demandas judiciais. O dano deve representar ofensa aos chamados direitos de personalidade, como à imagem e à honra, de modo a deses-

tabilizar psicologicamente o ofendido. V. A prática de *bullying* é ato ilícito, haja vista compreender a intenção de desestabilizar psicologicamente o ofendido, o qual resulta em abalo acima do razoável, respondendo o ofensor pela prática ilegal. VI. Aos pais incumbe o dever de guarda, orientação e zelo pelos filhos menores de idade, respondendo civilmente pelos ilícitos praticados, uma vez ser inerente ao pátrio poder, conforme inteligência do art. 932 do Código Civil. Hipótese em que o filho menor criou página na Internet com a finalidade de ofender colega de classe, atrelando fatos e imagens de caráter exclusivamente pejorativo. VII. Incontroversa ofensa aos chamados direitos de personalidade do autor, como à imagem e à honra, restando, ao responsável, o dever de indenizar o ofendido pelo dano moral causado, o qual, no caso, tem natureza *in re ipsa*. VIII. *Quantum* reparatório serve de meio coercitivo/educativo ao ofensor, de modo a desestimular práticas reiteradas de ilícitos civis. Manutenção do valor reparatório é medida que se impõe, porquanto harmônico com caráter punitivo/pedagógico comumente adotado pela Câmara em situações análogas. Apelos desprovidos” (TJRS, Apelação Cível 70031750094, rel. Liege Puricelli Pires, j. 30-6-2010).

“Apelação cível. Responsabilidade civil. Orkut. Aplicabilidade do CDC. Dano moral configurado. Perfil falso. Uso da imagem. 1. Aplicável à espécie as normas do Código de Defesa do Consumidor, pois as partes enquadram-se nos conceitos de consumidor e fornecedor de serviços, ainda que esses estejam estabelecidos a título gratuito, porquanto há ganho pela entidade demanda, ainda que de forma indireta. 2. O simples fato de ter sido utilizada indevidamente a imagem da autora e de pessoas de suas relações, familiares e amigos, pela clonagem efetuada, gera a ela danos à imagem que merecem ser indenizados, até por que a ré não comprovou ter retirado de imediato a clonagem ocorrida, ônus que lhe incumbia. 3. *Quantum* indenizatório mantido na forma fixada na sentença. 4. Honorários advocatícios em consonância ao art. 20, § 3º, do CPC. Manutenção. Recurso de apelação e recurso adesivo desprovidos, por maioria, vencido o revisor que dava provimento ao apelo e julgava prejudicado o recurso adesivo” (TJRS, Apelação Cível 70027841394, rel. Artur Arnildo Ludwig, j. 10-6-2010).

“Ação de indenização. Dano moral. Site de relacionamentos — Orkut. Perfil criado com intuito de denegrir a imagem da autora. Legitimidade passiva do réu. 1. Sentença que extinguiu o processo sem resolução de mérito, por entender que o réu (Google Brasil Internet Ltda.) não é parte legítima para compor o polo passivo da ação. Decisão que merece reforma. O réu é responsável na medida em que não adotou as medidas cabíveis para excluir, de imediato, do *site* de relacionamentos, o perfil criado única e exclusivamente para ofender a autora. 2. Possível a apreciação meritória, com base no permissivo do art. 515, § 3º, do CPC. 3. A prova dos autos

demonstra que, não obstante a autora tenha utilizado a ferramenta disponibilizada no próprio *site* para coibir a prática de abusos, o réu não tomou as providências devidas imediatamente, permitindo a manutenção das ofensas, dirigidas inclusive aos amigos da autora, para que os recados fossem passados à ela. O réu agiu com culpa, foi negligente, devendo, assim, responder pelos danos decorrentes da sua omissão. 4. Violação a direito de personalidade, de molde a atingir a honra e imagem da parte autora. Danos morais configurados. Recurso parcialmente provido” (TJRS, Recurso Inominado Cível 71002353613, rel. Eduardo Kraemer, j. 13-5-2010).

“Apelação cível. Ação de obrigação de fazer e não fazer c/c preceito cominatório e indenização por danos morais. Publicação de *site* na Internet com fotos da autora em momentos de intimidade com seu ex-namorado. Preliminares. Ilegitimidade passiva. Alegação de que o sítio foi hospedado em página da empresa matriz. Irrelevância. Demandada que exerce o ramo brasileiro da atividade de sua empresa-mãe. Tentativa de fruição da marca e dos serviços dessa, sem assunção dos ônus correlatos. Princípios do amplo acesso à justiça e da efetiva reparação dos danos causados ao consumidor. Precedente do STJ. Prefacial afastada. Cerceamento de defesa. Inocorrência. Matéria de fato suficientemente comprovada. Desnecessidade de produção de novas provas. Livre convencimento motivado do juiz da causa. Preliminar rechaçada. Mérito. Recorrente que, em seu provedor, hospeda *site* ofensivo à honra e à imagem da autora. Discussão restrita à obrigação reparatória. Relação de consumo configurada. Responsabilidade objetiva. Incidência da teoria do risco. Atividade que, apesar de lícita, é exercida sem maiores cuidados. Relaxamento dos procedimentos de segurança com vistas ao aumento da lucratividade. Criação de risco de forma consciente. Obrigação de responder por eventual desvirtuação do serviço. Quebra de nexo de causalidade pela atuação de terceiro. Inocorrência. Caracterização de fortuito interno, inábil ao afastamento da responsabilidade da ré. Precedentes do STJ. Obrigação de reparar configurada. *Quantum* indenizatório. Redução. Recurso conhecido e parcialmente provido” (TJSC, Apelação Cível 2007.038693-2, rel. Mônica Elias de Lucca Pasold, j. 12-4-2010).

“Apelação cível. Ensino particular. Ação indenizatória. Publicação em *site* jurídico de acórdão criminal onde vigora o segredo de justiça. Dano moral configurado. Dano reflexo. *Quantum*. Redimensionamento dos ônus sucumbenciais. Pedido de reforma que não ataca os fundamentos da sentença. Não conhecimento de parte do apelo. Cerceamento de defesa. Não configuração. I. Não se conhece de apelação genérica, que não ataca especificamente os fundamentos de fato e de direito que embasam o pedido de nova decisão. Desatendido, no caso concreto, o requisito intrínseco de admissibilidade da regularidade formal. Inteligência do art. 514, II, do Código de Processo Civil. Recurso do autor conhecido em parte. II. Ao Juiz — destinatário da

prova — incumbe aferir a necessidade, ou não, da produção de provas pelas partes, a teor do que determina o art. 130 do Código de Processo Civil. Inocorrência de cerceamento de defesa pelo julgamento antecipado da lide. Preliminar afastada. III. Ato ilícito configurado, no caso concreto, vez que agiu negligentemente a ré, instituição de ensino jurídico, ao publicar cópia de acórdão em sua página da Internet, não atentando para o fato de se tratar de ação com interesse de menor, em que se discutia crime contra os costumes, acabando por divulgar o nome completo das partes envolvidas e vindo, assim, a violar o direito de intimidade, imagem e vida privada dos envolvidos — violação ao art. 155, II, do CPC, por analogia, e art. 206 do Estatuto da Criança e do Adolescente. Dano moral *in re ipsa*. Dever de indenizar caracterizado. IV. Tem legitimidade o pai para, concorrentemente com o filho, pleitear danos morais em razão da publicação indevida de acórdão de processo criminal, em que este figura como vítima, em *site* jurídico, é o que se chama de dano reflexo. V. Na fixação do *quantum*, o Juízo tem de observar, segundo a melhor doutrina, o grau de culpa do ofensor; a capacidade econômica do responsável; a compreensão do responsável e o caráter pedagógico da condenação. Montante da condenação estabelecido na sentença, mantido, diante da capacidade econômica da ré. VI. Havendo o autor postulado danos morais em nome próprio, do filho e da mãe do menor, e logrado êxito, tão somente, quanto aos primeiros, há sucumbência recíproca, devendo os ônus sucumbenciais ser distribuídos nos termos do art. 21 do Código de Processo Civil. Sucumbência redimensionada no caso concreto. Preliminar afastada. Apelo do autor conhecido em parte e, na parte conhecida desprovido, e apelo do réu parcialmente provido” (TJRS, Apelação Cível 70032292864, rel. Liege Puricelli Pires, j. 18-3-2010).

“Ação de Indenização. Rito sumário. Página do Orkut invadida por menor infrator, com modificação de dados e inserção de palavras ofensivas à dignidade da autora, promovendo a troca de senha de modo a impedir o acesso para remoção das ofensas. Google Brasil Internet Ltda., que faz parte do mesmo grupo empresarial da Google, Inc., que administra o Orkut. Responsabilidade objetiva. Aplicabilidade do CODECON, considerando que a apelante é remunerada de forma indireta no *site* da Internet. Ainda que assim não fosse, presentes os pressupostos da responsabilidade subjetiva: o dano, a culpa e o nexo de causalidade. A demora do Google em remover a página do ar representa uma conduta omissiva culposa, estando, pois presente a responsabilidade de reparar pelo dano sofrido. Correta a sentença. Não provimento do apelo” (TJRJ, Apelação 0115539-94.2009.8.19.0001 (2009.001.62742), rel. Galdino Siqueira Netto, j. 23-2-2010).

“Responsabilidade civil. Dano moral. Uso indevido da imagem. Fotos íntimas. I. Tendo sido demonstrado o comportamento negligente dos réus que repassaram as

imagens sem a autorização da demandante, dando causa a sua propagação, é evidente o dever de indenizar. Exegese do art. 20 do CC/2002. Hipótese na qual foram divulgadas na Internet e através de correio eletrônico fotos íntimas da autora. II. É de ser majorado o montante indenizatório arbitrado em sentença. A indenização visa a reparação do dano sofrido sem acarretar, por outro lado, a possibilidade de enriquecimento sem causa. Indenização fixada em R\$ 24.000,00, consoante os parâmetros utilizados por esta Câmara Cível em situações análogas. Solidariedade passiva dos demandados reconhecida. Apelação dos réus desprovida. Apelação da autora provida” (TJRS, Apelação Cível 70027861202, rel. Túlio de Oliveira Martins, j. 26-11-2009).

“Danos morais. Veiculação de imagem pejorativa na Internet, produzida mediante montagem. Valor da indenização que merece majoração por demasiadamente reduzido. Absoluta carência de informações, contudo, a amparar a pretensão da parte autora. Recurso parcialmente provido” (TJRS, Recurso Inominado Cível 71001966126, rel. Vivian Cristina Angonese Spengler, j. 7-10-2009).

“*Responsabilidade civil. Indenização por danos morais. Site de relacionamentos Orkut. Ofensa à honra e moral. Ausência de responsabilidade do provedor de hospedagem.* O provedor de hospedagem não responde pelo conteúdo das informações armazenadas, exceto quanto à eventual responsabilidade subjetiva decorrente de negligência pela não solicitude quando da retirada dessas informações de suas páginas. Apelação provida” (TJPR, Apelação Cível 0572155-9, REL. Nilson Mizuta, j. 21-1-2009).

“*Apelação cível. Divulgação sem autorização, via Internet, de fotos íntimas. Dever de indenizar. Litigância de má-fé. Inocorrência.* 1. A divulgação, via Internet, de fotografias de momentos íntimos da autora sem a sua autorização constitui ato ilícito e enseja o dever de indenizar. 2. Quanto à caracterização do dano moral, em casos como o dos autos, a ocorrência é *ipso facto*. A prova do dano é dispensável. Situação como a presente dispensa demonstração de espécie alguma, pois o fato fala por si, já que a veiculação de imagens em momentos íntimos, envolvendo a identificação do telefone e nome da vítima, acarreta, sem dúvida, abalo à honra e à dignidade pessoal desta. 3. Tratando-se de dano moral, o conceito de ressarcimento abrange duas forças: uma de caráter punitivo, com vistas a castigar o causador do dano pela ofensa praticada e outra de caráter compensatório, destinada a proporcionar à vítima algum benefício em contrapartida ao mal sofrido. Assim, tal ressarcimento presta-se a minimizar o desequilíbrio e aflição suportados pela vítima, não podendo, em contrapartida, constituir fonte de enriquecimento injustificado. 4. Para a configuração da litigância de má-fé, com a consequente aplicação dos arts. 17 e 18 do CPC, é imprescindível que se prove, de forma cabal, que a parte estava agindo

imbuída de dolo processual, o que não se verificou no caso dos autos” (TJMG, Recurso 1.0109.07.009368-6/001(1), rel. Wagner Wilson, j. 19-8-2009).

“*Mandado de segurança. Procedimento administrativo. Ministério da Cultura. Divulgação de informações na Internet. Violação do direito à imagem. Atributo. Sentença confirmada.* 1. A atitude da Administração Pública em divulgar no site do Ministério da Cultura peças dos procedimentos administrativos que envolvem os impetrantes, sem disponibilizar conjuntamente os argumentos de defesa, viola o direito à imagem — atributo da apelada. 2. Apelação da União e remessa oficial improvidas” (TRF01, AMS 2001.34.00.004203-1/DF, rel. Selene Maria de Almeida, publ. 31-7-2009).

“Dano moral. Uso indevido do nome da reclamante em sítio da Internet. Prova. O sofrimento não depende de prova, é da natureza humana em determinadas circunstâncias. O que depende de prova são os fatos que o provocam, e no caso, o uso indevido do nome da reclamante, profissional cuja carreira se assenta justamente sobre seus conhecimentos (...). Por já estar desligada da empresa, colocou em risco justamente essas qualidades e evidentemente lhe causou desassossego, apreensão e dor” (TRT2, RO 00575200707202000, rel. Silvana Abramo Margherito Ariano, j. 10-3-2009).

“Responsabilidade civil. Empregador. Uso indevido de imagem do empregado. Veiculação não autorizada de fotografia do empregado no sítio da empresa na Internet. Inexistência de autorização do empregado. Danos materiais não caracterizados. Danos morais configurados. Desnecessidade de demonstração dos prejuízos. Reparabilidade assegurada constitucionalmente (CF, art. 5º, X). Precedentes. Indenização. Arbitramento segundo critérios genéricos, com livre apreciação do juiz e mediante devida cautela. Redistribuição dos ônus da sucumbência. Aplicação do art. 21, *caput*, do CPC. Recurso de apelação da empresa ré provido em parte, e provido o recurso adesivo do autor” (TJSP, Apelação 389.824-4/3-00, rel. Des. Ariovaldo Santini Teodoro, j. 23-9-2008).

“*Responsabilidade civil. Suposta violação a direitos autorais. Apostila. Indenização buscada.* Compilação de textos extraídos da Internet, cuja montagem sequer restou demonstrada como sendo de autoria do autor. Apostila solicitada pela escola e sem fins comerciais. Indenização indevida. Apelação desprovida” (TJRS, Apelação Cível 70024951303, rel. Des. Marilene Bonzanini Bernard, j. 17-12-2008).

“*Agravo. Retirada de site do servidor de hospedagem. Disponibilidade de material gratuitamente. Ofensa a direito autoral do autor. Dano de difícil reparação. Fornecimen-*

to de dados dos criadores da página de Internet. Ausência de urgência. Indeferimento. Deve ser deferida a antecipação de tutela para retirar do servidor de hospedagem da Internet página eletrônica que disponibiliza material e produto de autoria do autor, em razão da possibilidade de ocorrência de dano de difícil reparação. Ausente a demonstração da urgência, do fundado receio de dano irreparável ou de difícil reparação, impõe-se o indeferimento da tutela antecipada quanto ao fornecimento de documentos sobre os criadores da página da Internet atacada, devendo-se observar o regular prosseguimento do feito” (TJMG, Agravo 1.0024.08.037843-3/00, rel. Alvimar de Ávila, DJ 12-7-2008).

“Civil e consumidor. Internet. Relação de consumo. Incidência do CDC. Gratuidade do serviço. Indiferença. Provedor de conteúdo. Fiscalização prévia do teor das informações postadas no site pelos usuários. Desnecessidade. Mensagem de conteúdo ofensivo. Dano moral. Risco inerente ao negócio. Inexistência. Ciência da existência de conteúdo ilícito. Retirada imediata do ar. Dever. Disponibilização de meios para identificação de cada usuário. Dever. Registro do número de IP. Suficiência. 1. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei n. 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo ‘mediante remuneração’, contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. 3. A fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na *web* por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o *site* que não examina e filtra os dados e imagens nele inseridos. 4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no *site* pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/2002. 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do *site*, sob pena de responsabilização subjetiva por culpa *in omissendo*. 7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo que registra o número de protocolo (IP) na Internet dos computadores utilizados para o cadastramento de cada conta mantém

um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de Internet. 8. Recurso especial provido” (STJ, REsp 1.186.616/MG, 3ª Turma, rel. Ministra Nancy Andrigli, j. 23-8-2011, DJe 31-8-2011).

“Apelação cível. Ação de indenização cumulada com condenatória a obrigação de fazer. Internet. Google. Orkut. Criação de perfil falsamente atribuído ao autor. Provedor de hospedagem. Responsabilidade objetiva. Aplicação do Código de Defesa do Consumidor. Responsabilidade inerente à natureza da atividade desenvolvida. Nomeação à autoria. Dever do réu. Danos morais convertidos em indenização por perdas e danos decorrentes da falta de nomeação. Recurso provido. 1 — O Google, responsável pelo *site* de relacionamentos denominado Orkut, está sujeito ao Código de Defesa do Consumidor nas relações com seus usuários. 2 — O Orkut é um provedor de serviço de Internet que se caracteriza pela hospedagem de páginas pessoais de usuários, possibilitando a troca de mensagens e a criação de comunidades, que ganham adeptos conforme interesses, ideias ou curiosidades comuns. (...) 4 — O Google responde de forma objetiva pelo provedor de hospedagem e pela confidencialidade dos dados dos seus usuários, mas não pelo conteúdo inserido em cada perfil individual. 5 — É impossível a retirada de conteúdo da rede sem a provocação da parte interessada, diante da inviabilidade técnica, fática e jurídica de o provedor de hospedagem varrer seus servidores à procura de um determinado tipo de informação. 6 — A criação de perfil falsamente atribuído ao Autor somente pode ser aferida pelo próprio ofendido, pois a eficiência dos mecanismos de filtragem de conteúdo inseridos no Orkut depende de indicação precisa da parte interessada. 7 — O Google possui meios adequados à identificação do usuário do Orkut que pratique eventual ilegalidade, promovendo o eficiente rastreamento dos usuários infratores, impedindo, assim, o anonimato, diligência razoável imputada a um provedor de conteúdo de Internet. 8 — O Google detém o perfil do Orkut em nome alheio, já que a propriedade da coisa (conteúdo do perfil) é do próprio usuário. 9 — Competia ao Google ver a nomeação à autoria do verdadeiro criador do perfil ofensivo ao Autor. A omissão, existente sentença de mérito, impõe ao Réu o dever indenizatório ao Autor. 10 — Recurso não provido” (TJMG, Apelação Cível 1.0024.10.045653-2/002, rel. Des. José Marcos Vieira, j. 11-5-2011).

“Civil e processual civil. Mensagens ofensivas à honra do autor veiculadas em rede social na Internet (Orkut). Medida liminar que determina ao administrador da rede social (Google) a retirada das mensagens ofensivas. Fornecimento por parte do ofendido das URLs das páginas nas quais foram veiculadas as ofensas. Desnecessidade. Responsabilidade técnica exclusiva de quem se beneficia da ampla liberdade de acesso de seus usuários. 1. O provedor de Internet — administrador de redes sociais —, ainda em

sede de liminar, deve retirar informações difamantes a terceiros manifestadas por seus usuários, independentemente da indicação precisa, pelo ofendido, das páginas que foram veiculadas as ofensas (URLs). 2. Recurso especial não provido” (STJ, REsp 1.175.675/RS, 4ª Turma, rel. Min. Luis Felipe Salomão, j. 9-8-2011, *DJe* 20-9-2011).

“Agravamento regimental em agravo de instrumento. Responsabilidade civil. Indenização por danos morais. Publicação de matérias vexatórias e sensacionalistas em site da Internet. 1. O Tribunal de origem, procedendo com amparo nos elementos de convicção dos autos, constatou a conduta ilícita do jornalista e reconheceu o seu dever de indenizar a agravada pelos danos morais sofridos. 2. Diante da falta de parâmetros objetivos para fixar o valor indenizatório, foram observados os seguintes elementos: gravidade e extensão do dano, reincidência do ofensor, posição profissional e social do ofendido, e condição financeira do ofensor e da vítima. 3. Portanto, os danos morais fixados pelo Tribunal de origem em quantia irrisória, foram majorados por esta Corte Superior, com vistas a que o valor da indenização por danos morais atendessem ao binômio ‘valor de desestímulo’ e ‘valor compensatório’. Agravo regimental não provido. (STJ, AgRg no Ag 1.072.844/SC, 4ª Turma, rel. Ministro Luis Felipe Salomão, j. 17-5-2011, *DJe* 20-5-2011).

“Responsabilidade civil. Danos Morais. Perfil e comunidade falsa, com conteúdo difamatório e pejorativo hospedadas em site de relacionamento (Orkut). Ré tomou ciência inequívoca da ilicitude dos conteúdos, por meio eletrônico, e quedou-se inerte. Inocorrência de dúvidas quanto à ilicitude do fato. Providência administrativa que dispensaria determinação judicial. Sentença de parcial procedência determinando à ré informar o IP do responsável pela criação das páginas, além de condená-la ao pagamento de indenização por danos morais no importe de 30 salários mínimos, mais honorários de sucumbência a razão de 10% sobre o valor da condenação. (...)” (TJSP, Apelação 0214748.35.2009.8.26.010, rel. Des. James Siano, j. 9-11-2011).

“Obrigação de fazer. O banco tomou conhecimento do envio de mensagem eletrônica ilícita (*e-mail*), enviada em nome do empregado de nome A.F. por possível *hacker* (anônimo) com intuito de prejudicá-lo, a outros funcionários e, inclusive, ao banco. Devem os provedores de serviços utilizar meios tecnológicos e equipamentos informáticos que possibilitem a identificação dos dados de conexão dos usuários, para que tais informações sejam disponibilizadas a quem de direito, em caso de ato ilícito, pois nem sempre os dados cadastrais contendo os nomes e endereços e demais danos pessoais dos usuários estarão corretos ou atualizados.

Como corolário do princípio da dignidade da pessoa humana, a Constituição Federal assegurou o direito à intimidade, proclamando no art. 5º, XII, a inviolabilidade do sigilo das comunicações telegráficas de dados e telefônicas; apesar da magnitude do direito em destaque, de cunho constitucional, é sabido que as liberdades públicas estabelecidas não podem ser consideradas como tendo valor absoluto, cedendo espaço para as hipóteses em pessoas escondendo no anonimato utilizam-nas para acobertar a prática de atividade ilícita, devendo o provedor da Internet ser obrigado a prestar as informações necessárias e suficientes. Art. 461 do CPC. Descabe a execução específica através do mecanismo previsto pelo art. 461 do CPC, em virtude da obrigação de prestar as informações requeridas pelo Autor. Obrigação de fazer que se resolve em perdas e danos, que corretamente e de forma razoável foram arbitrados em R\$ 20.000,00 (vinte mil reais), corrigidos. Recurso não provido. (...)” (TJSP, Apelação 0135762-07.2008.8.26.0002, rel. Des. Paulo Hatanaka, j. 4-10-2011).

6 — A MARCA NA INTERNET

REGISTRO DE DOMÍNIOS NA INTERNET

Comentários:

Os domínios são os endereços eletrônicos da *web*. Tem-se entendido que o domínio é a extensão e a representatividade da marca na Internet. Em casos de disputa de domínios, os Tribunais têm dado preferência às marcas que detêm registro no Instituto Nacional de Propriedade Industrial — INPI. Claro que há exceções, visto que, diferentemente do registro de marca pelo qual é possível classificar por ramo de atividade, o domínio é um só. Então, dependendo do caso, é preciso analisar quem teria maior necessidade de ter o domínio, e a solução se passa pelo direito consumerista, de não gerar “confusão na cabeça do consumidor”. Uma pequena empresa precisa sempre pesquisar se a marca está protegida ou não, antes de fazer o registro do domínio. Ainda é comum registrar o domínio e esquecer de registrar a marca.

“Apelação cível. Ação de indenização c/c obrigação de fazer. Registro de domínio de Internet. Registro da marca no INPI. Direito de uso que abrange o comércio eletrônico e o domínio. Ofensa ao direito de propriedade configurada. Não se pode deixar de garantir o uso da marca a quem tiver o respectivo registro junto ao INPI, pois este passa a deter todos os direitos decorrentes de tal ato, inclusive a divulgação da marca via Internet” (TJMG, Recurso Cível 01681161.0672.02.083567-0/001(1), rel. Valdez Leite Machado, j. 5-8-2010).

“Apelação cível. Internet. Propriedade industrial. Ação objetivando a cessão do nome de domínio na Internet. Compatibilização e interpretação sistemática dos diplomas legais e normas constitucionais vigentes. 1. Não se conhece do agravo retido interposto pelo recorrente, porquanto não reiterado em suas razões recursais. 2. A controvérsia posta nos autos limita-se a definição se o registro da marca ‘OI’, formalizado pela autora em 22-7-1993 e registrado em 5-9-1995 junto ao INPI, deve ou não prevalecer sobre o registro dos domínios na Internet: oiamigos.com.br; oicard.com.br; oiclube.com.br; oivisa.com.br; oibancoInternet.com.br; oibank.com.br; oibanking.com.br; oibus.com.br; oicliente.com.br; oivisacard.com.br; oivisao.com.br, levado a cabo pela ré na Nic.br. 3. É sabido que, no mercado de consumo atual, uma empresa é reconhecida e individualizada pelos sinais de identificação adotados e que se agregam a sua reputação e patrimônio. 4. Hodiernamente, pode-se perceber que tais elementos identificadores não se limitam à

marca e ao nome comercial, em razão do crescente avanço tecnológico da Internet para a aquisição de produtos e serviços. 5. O princípio da especialidade rege o sistema de concessão de marcas no país, harmonizando a convivência de marcas semelhantes ou idênticas, desde que atreladas a serviços e produtos que não se identifiquem. 6. Porém, em se tratando de domínio na Internet, não é a matéria orientada pelo princípio da especialidade e a legislação que trata da matéria é ainda incipiente, trazida em resoluções e não disciplinando questões mais complexas e ultimamente recorrentes em demandas jurídicas. 7. A Resolução n. 001/98 regulamentou o registro do domínio e instituiu o princípio da primazia do registro (“first to file”), adotando como critério o princípio de que o direito ao nome do domínio será conferido ao primeiro requerente que satisfizer, quando do requerimento, as exigências para o registro do nome. 8. Conquanto não exista normatização a respeito se o nome de domínio deve receber o mesmo tratamento jurídico utilizado para o registro de marcas e nomes comerciais, notadamente no que concerne a registrabilidade de nomes que, embora não sejam idênticos, arremedam a outros já registrados, o princípio da primazia do registro não deve receber interpretação isolada. 9. As resoluções atinentes ao registro de domínios devem ser compatibilizadas com outros institutos e princípios do direito pátrio, notadamente aqueles que regulamentam a propriedade intelectual, como forma de coibir práticas prejudiciais às relações de consumo e de concorrência desleal. 10. A variação nominativa da marca ‘OI’, utilizada pela ré para registro de domínio de Internet, sem sombra de dúvidas, induz os consumidores a erro, na introdução de elementos semelhantes à marca da autora, por associação, criando risco aos usuários da rede que não se atentam para a diferença do conjunto e prejudicando a atividade da recorrida, cujo elemento identificador é perfeitamente conhecido publicamente no mercado. 11. A Resolução n. 001/98 do Comitê Gestor da Internet deve ser interpretada de forma sistemática, de modo que o princípio da primazia do registro seja compatibilizado com os casos em que já existam marcas já devidamente registradas no INPI, impedindo-se, assim, o registro do domínio que se pretende levar a cabo. 12. Não pode uma resolução negar vigência a Lei de Propriedade Industrial e a própria Constituição da República, que não só protege o direito à propriedade da marca como também garante proteção aos demais signos distintivos. 13. Desprovisionamento do recurso” (TJRJ, 8ª Câmara Cível, Apelação 0168116-20.2007.8.19.0001 (2009.001.68741), rel. Monica Costa di Piero, j. 29-6-2010).

“Propriedade industrial. Nome de domínio que não pode afrontar o direito à marca de terceiro, sobretudo quando há similitude de atividades entre as empresas disputantes, pena de se caracterizar concorrência desleal. Pendência de análise administrativa que não obsta o pronunciamento judicial. Recurso desprovido” (TJSP, Apelação 994.09.323085-6, rel. Des. Roberto Solimene, j. 22-7-2010).

*“Direito processual civil. Agravo de instrumento. Tutela antecipada. Conflito entre o uso da marca e do nome de domínio eletrônico. Pedido de suspensão do uso dos sítios eletrônicos. Princípio da primazia do registro. Exceções não identificadas. Cognição sumária. Inexistência dos requisitos do art. 273, do CPC. A marca, desde que registrada de acordo com a Lei da Propriedade Industrial (LPI), goza de proteção jurídica no Brasil, procurando evitar que a marca seja utilizada por terceiros de forma indevida ou sem autorização, mas a legislação pertinente não abrange expressamente os nomes de domínio. Quanto ao nome de domínio, no Brasil foi consagrado o princípio do *first-to-file* (princípio da primazia do registro) no tocante ao registro de domínio, conforme redação do art. 1º da Resolução n. 2/2008 do CGI — Comitê Gestor da Internet no Brasil. Esta regra comporta exceções, mas não são vislumbradas no caso *sub judice*, ao menos em sede de cognição sumária, razão pela qual se indefere o pedido de suspensão do uso dos sítios eletrônicos, em sede de tutela antecipada”* (TJMG, Recurso Cível 0083321-47.2010.8.13.0000, rel. Mota e Silva, j. 27-4-2010).

*“Direito privado. Propriedade industrial. Marca. Nomes de domínio. Nome fantasia. Adjudicação. Cancelamento. 1. A proteção à propriedade da marca não se esgota nos interesses meramente individuais de seu titular, representando verdadeiro mecanismo de defesa do consumidor e inibição da concorrência desleal, visando a resguardar ‘o interesse social e o desenvolvimento tecnológico e econômico do País’ — art. 5º, XXIX, da Constituição Federal. Revela-se crucial, portanto, para o atendimento dos preceitos da Constituição Federal, a expansão da proteção conferida pela Lei n. 9.279/96, fazendo-a abranger não só ‘o uso da marca em papéis, impressos, propaganda e documentos relativos à atividade do titular’, mas também a sua utilização na confecção de nomes de domínio para a utilização no crescente e promissor mercado virtual. 2. Constatada a similitude, a identidade entre os produtos e serviços abrangidos pela classe em que registrada a marca da 1ª autora e o objeto social da ré, evidenciando a possibilidade real e concreta de indução de terceiros a erro, deve ser acolhido o pedido de abstenção de utilização de nome de domínio (DNS — *Domain Name System*) que contenha o designativo de marca registrada e utilizada em tempo pretérito, bem como de nome fantasia que o reflita. Recurso não provido. 3. A ilegalidade do registro do nome de domínio, nas condições descritas acima, autoriza a determinação de seu cancelamento, um dos desdobramentos do pedido de adjudicação. Recurso provido em parte”* (TJMG, Recurso Cível 3076931-02.2008.8.13.0672, rel. Vagner Wilson, j. 2-12-2009).

“Apelação cível. Propriedade industrial. Marca notoriamente conhecida. Art. 126 da Lei n. 9.279/96. Domínio de endereço de internet. Comitê gestor de internet no Brasil. Resolução n. 8/2008. possibilidade de cancelamento por ordem judicial. A Reso-

lução n. 8/2008 do Comitê Gestor de Internet no Brasil prevê a possibilidade de cancelamento de domínio apenas por ordem judicial. Sendo caso de marca notoriamente conhecida, plenamente razoável o pedido de transferência do domínio. Sucumbência redimensionada. Art. 20 do CPC. Dever do vencido. Apelação provida” (TJRS, Apelação Cível 70029767530, rel. Marilene Bonzanini Bernardi, j. 30-9-2009).

*“Apelação cível. Direito privado não especificado. Propriedade industrial. Uso indevido de domínio. Concorrência desleal configurada. 1. Registro de domínios foneticamente idênticos na internet. Concorrência desleal configurada. A questão cinge-se à verificação da prática de concorrência desleal ante o fato de a empresa ré registrar domínio na Internet foneticamente idêntico ao da empresa autora para venda de mesmo tipo de produto, fazendo com que os usuários que objetivavam o sítio da demandante fossem remetidos ao domínio da empresa ré. 2. Critério da anterioridade. Art. 1º da Resolução n. 2/2005. Em se constatando que a empresa autora, efetivamente, registrou o domínio anteriormente à empresa ré, é indubitável que essa última agiu em concorrência desleal em relação àquela, porquanto atribuiu um domínio (*tecnospray.com.br*) que não tem relação alguma com o nome através do qual é conhecida no mercado, mas que guarda profunda semelhança na grafia e na pronúncia com o domínio registrado por outra empresa concorrente. 3. Danos materiais não comprovados. A demonstração do prejuízo ou da redução patrimonial motivadora do pagamento da indenização deveria ter sido feita ao menos, *in casu*, com prova de quantos acessos indevidos ocorreram através do domínio da ré (que objetivavam, na realidade, o acesso aos produtos da autora); ou, ainda, se a autora teria tido redução nas vendas em razão dos problemas decorrentes dos domínios com registros similares. Por conseguinte, não comprovados os danos materiais, não há dever indenizatório, e obstaculiza, inclusive, que os respectivos prejuízos sejam apurados em fase de liquidação de sentença. Apelação desprovida. Recurso adesivo parcialmente provido”* (TJRS, Apelação Cível 70024891277, rel. Odone Sanguiné, j. 10-12-2008).

“Propriedade industrial. Uso de domínio virtual. Uso de subdomínio idêntico ao domínio principal da autora. Proteção da L. 9.279/96. Uso indevido na Internet de nome alheio. Proteção ao nome devidamente registrado. Manifesta intenção de usurpar nome e prestígio alheios, configurando concorrência desleal. Bloqueio do domínio principal da ré determinado de ofício, ao longo da instrução processual. Indevida compensação dos prejuízos sofridos pela autora e ré, adotada na sentença. Ausência de conduta ilícita da autora, bem como nexo de causalidade entre sua conduta e os danos eventualmente sofridos pela ré. Inexistência de pedido contra-

posto ou reconvenção que legitimasse a condenação implícita da autora. Critérios para a apuração do *quantum* da condenação. Art. 210 da Lei de Propriedade Industrial. Ação parcialmente procedente. Recurso provido” (TJSP, Apelação 473.265.4/9-00, rel. Des. Francisco Loureiro, j. 18-12-2008).

“*Agravo de instrumento*. Propriedade industrial. Nome de domínio da Internet. Abstenção. Pedido de liminar específica para o fim de impedir a ré agravada de usar o nome ‘megashop’ sob qualquer forma (Lei n. 9.279/96, art. 209, § 1º). Confusão com a Marca ‘meggashop’, da Agravante, com registro regular no INPI. Possibilidade. Presentes os requisitos para a concessão da liminar específica (...) de rigor a concessão da tutela de urgência. (...)” (TJRJ, Apelação 2008.001.16030, rel. Maria Inês da Penha Gaspar, j. 9-4-2008).

“*Agravo retido*. Inobservância do disposto no art. 523, § 1º, do CPC. Não conhecimento do recurso. Apelação cível. Reconvenção. Inexistência de conexão com o pedido da ação principal. Registro de domínio de internet. Registro da marca no INPI. Direito de uso que abrange o comércio eletrônico e o domínio. Ofensa ao direito de propriedade configurada. (...) O uso de nome ou marca em domínios na Internet sem a autorização do proprietário, que detém registro anterior no INPI, configura ato ilícito” (TJMG, Apelação Cível 1.0439.03.021925-7/001, rel. Valdez Leite Machado, j. 23-4-2008).

SITES DE BUSCA — ADESÃO PATROCINADA COM NOME DO CONCORRENTE

Comentários:

Os chamados “links patrocinados” surgiram com a sofisticação dos mecanismos de busca e estão intimamente ligados ao conceito de concorrência desleal. Trata-se da associação de nomes a marcas de terceiros, fazendo com que, todas as vezes que houver a busca por aquele termo, apareça automaticamente uma oferta do contratante dos links ao lado do resultado da busca. Assim, sempre haverá a “lembrança” de outro endereço eletrônico quando quisermos fazer a busca de determinado assunto.

“Site de busca. Desvio de clientela. Empresa multinacional. Inserção de domínio de empresa de porte pequeno. Concorrência desleal. Direito a indenização. Civil. Processo Civil. Comercial. Constitucional. Internet. Sítios de busca. Marketing.

Provedora de acesso e empresa comercial poderosas. Multinacionais. Empresa nacional de porte significativamente inferior. Publicidade. Abuso de direito. Concorrência desleal. Desvio de clientela. A Internet passou a preencher e ocupar um importante espaço na vida das pessoas. Pouco falta para que não se a encare, mais, como um ‘mundo virtual’, mas real, tantas as implicações e ressonâncias na vida moderna. A autora é uma sociedade empresária especializada em comércio eletrônico, detentora de loja exclusivamente virtual que disponibiliza produtos para crianças e adolescentes, tais como brinquedos, livros, DVD, jogos eletrônicos etc. A segunda ré, de muito maior porte, comercializa os mesmos produtos, dentre uma enorme gama de outros artigos. A primeira ré, empresa multinacional, das mais poderosas do planeta, tem, dentre outras atividades industriais e científicas na área da informática, um sítio de buscas para assinantes e clientes. Contrato celebrado entre as rés que insere no âmbito da publicidade da segunda ré, o domínio da autora, fazendo com que os clientes e usuários em geral cheguem aos mesmos produtos e ao próprio domínio da autora através apenas do domínio da primeira ré, concorrente específica daquela. Embora o domínio da autora faça alusão à figura do ‘Saci Pererê’, do folclore nacional, tornando-a insusceptível de dominação exclusiva, a menção no domínio existente no âmbito da Internet garante proteção ao titular do domínio cujo depósito, ademais, já foi depositado junto ao INPI. Quadro probatório. Recusa das rés quanto ao fornecimento de cópia do contrato celebrado entre as mesmas. Sites patrocinados. Alegação de contrato verbal. Inconsistência. Prática evidente de marketing abusiva. A análise mais razoável do esquema engendrado pelas rés demonstra a ocorrência da abusividade, a mais evidente. A vinculação do domínio da autora ao sítio da poderosa multinacional que com ela concorre, de forma quase subalterna, certamente angaria a clientela já potencialmente da autora, de menor porte e a causar maiores dificuldades no enfrentamento desigual. Desvio de clientela inegável. Constitui concorrência desleal qualquer ato de concorrência contrário aos usos honestos em matéria industrial e comercial. A livre concorrência consubstancia um princípio geral da atividade econômica, constitucionalmente assegurado (cf. art. 170, IV, CRFB/88). Recurso a que se nega provimento” (TJRJ, Apelação 0147301-07.2004.8.19.0001 (2008.001.60797), rel. Mario Assis Gonçalves, j. 7-4-2009).

“Antecipação de tutela. Concorrência desleal. Utilização indevida do nome e marca da Autora como termo para pesquisa em anúncios veiculados em páginas da Internet. Determinada a abstenção do uso do nome da autora em sítios de busca. Admissibilidade. Presença dos requisitos necessários para a concessão da tutela. Recurso improvido” (TJSP, Agravo 555.448-4, rel. Des. Vito Guglielmi, publ. 15-5-2008).

Comentários:

É muito fácil copiar uma imagem da Internet, inclusive as marcas. Dessa forma, também é muito fácil reproduzir essa marca copiada em outros locais, sobretudo de forma indevida. A marca é o ativo intangível mais valioso de uma empresa. Por isso, ela deve monitorar periodicamente a Internet, para ver como está a “Reputação da Marca Digital”, quais conteúdos estão associados a ela, se há alguém parasitando a marca, especialmente nas redes sociais.

Mas, dependendo da situação, caso envolva funcionário, consumidor, parceiro, deve-se ter cuidado com as medidas legais a tomar, para não piorar o caso. É recomendável sempre tentar primeiro uma solução amigável, entrando em contato direto com quem está fazendo o uso indevido, especialmente se envolver consumidor.

“(…) 3. Danos morais. A ex-empregada, ora recorrente, criou no Orkut a página ‘Senzala Zest’, em cuja descrição se apresenta destinada a ‘todos aqueles que são ou já foram escravos do Restaurante Zest’ (fl. 24). É incontroverso que a ex-empregada criou a página, como também que por ali foram manifestadas várias agressões, como a condição de trabalho escravo (já presente no nome da página), como também a suposta homossexualidade do filho do sócio, ou ainda a desqualificação profissional responsável para lhe atribuir a condição de ‘cozinheira de sopão’. A criação da chamada ‘comunidade’ produtora de fatos lesivos já é, em si mesma, ato lesivo à honra. Presentes os requisitos que justificam o dever de indenizar (arts. 186 e 187 do Código Civil). O empregado, criador e moderador de comunidade em sítio de relacionamento (Orkut), que permite a veiculação de conteúdo com potencial ofensivo contra o empregador, está sujeito a responsabilidade civil” (TRT02, Processo 00266-2007-022-02-00-3, rel. Rafael E. Pugliese Ribeiro, j. 30-3-2010).

‘Apelação cível. Responsabilidade civil. Direitos autorais. Fotografias. Utilização em livro de receitas. Disponibilização na Internet, sem prévia autorização. Dano moral. Dever de indenizar. Sendo disponibilizadas, em site do clube, fotografias destinadas a livro de receitas do réu, sem autorização do seu autor, impõe-se o dever de indenizar pelo dano moral, nos termos do disposto no art. 108 da Lei n. 9.610/98, na medida em que depende de autorização prévia e expressa do autor a utilização da obra, por quaisquer modalidades. *Dano moral. Manutenção do quantum estabelecido pela sentença.* De ser mantido o valor arbitrado na sentença pelos danos morais (20 salários mínimos), tendo em vista que observados, quando da fixação, os princípios

da proporcionalidade e razoabilidade. *Dano patrimonial. Indenização. Cabimento. Apuração em liquidação de sentença.* Cabível a indenização pelos danos materiais pelo simples fato de o réu ter se utilizado das fotografias destinadas a livro de receitas sem a devida autorização, as quais foram inseridas no site do clube, com propósito de publicidade e propaganda, encobrendo interesse econômico na divulgação da marca e produtos e fazendo propaganda da Confraria U.C., com o intuito de vender ingressos para os jantares por ela produzidos. *Quantum a ser estabelecido em liquidação de sentença por arbitramento.* Aplicação do art. 475-C do CPC. Orientação doutrinária e jurisprudencial do STJ e desta Corte Estadual. Primeira apelação desprovida e segunda apelação parcialmente provida” (TJRS, Apelação Cível 70031905714, rel. Tasso Caubi Soares Delabary, j. 7-4-2010).

“Propriedade industrial. Apelação cível. Registro de marca. Aplicação do art. 124, XXIII, da LPI. Utilização pela apelante de imagem da empresa-apelada. Concorrência desleal. Condenação no ônus da sucumbência. Cabimento. Incidência do art. 20 do CPC. Arquivamento do registro anulando em virtude do cumprimento do contrato assinado por advogado sem procuração nos autos. 1 — Recurso no qual se discute se há possibilidade de confusão ao público consumidor na coexistência da marca mista ‘FUBU’ (Registro 820.089.370), classe 25:10-20-60, de titularidade da empresa-apelante, Bonés Pointer Ltda. ME., com as marcas mistas ‘FUBU’ (Registro 820.460.931), classe 25:10-20-30 e ‘FB’ (Registro 820.460.923), classe NCL (7) 25, de titularidade da empresa-apelada, GTFM INC.; 2 — Impossibilidade de coexistência das marcas em cotejo, ante todo um conjunto probatório que demonstra claramente que as marcas possuem identidade gráfica e se destinam a distinguir produtos ou serviços idênticos, semelhantes e afins, suscetíveis de causar confusão ao público consumidor, alcançando o mesmo segmento mercadológico; 3 — A má-fé da apelante restou caracterizada através da verificação do documento de fls. 158 que é o layout da página da Internet da empresa-apelante (www.fubuwear.com.br), que foi criada com a imagem dos idealizadores e fundadores da empresa-apelada (fls. 120), revelando que a apelante tinha pleno conhecimento da existência das marcas da apelada e efetivamente copiou não só o próprio nome da marca, mas também toda a ideia, chegando ao ponto de utilizar a referida foto com o fim de aproveitar a fama e a credibilidade das marcas da apelada, incidindo no art. 124, XXIII, da LPI e caracterizando a concorrência desleal; 4 — Incabível a pretensão da apelante no sentido de ser excluída da condenação em custas e honorários advocatícios, ante o princípio da sucumbência adotado pelo nosso sistema processual e consagrado no art. 20 do CPC; 5 — O arquivamento da marca anulanda ocorrido em 5-9-2006 não altera a situação em concreto, uma vez que à época da prolação da sentença, em 27-3-2001, o registro anulando encontrava-se em plena vigência, cabendo o reexame da causa tal como foi julgada pela inferior instância, notadamente no caso em tela onde, em que o arquivamento do registro anulando se deu

em virtude do cumprimento da cláusula n. 02 do acordo celebrado entre as empresas e que não foi homologado judicialmente em virtude da não formalização da representação processual do advogado que assinou o acordo pela empresa-apelante, Bonés Pointer Confeções Ltda. ME; 6 — Apelação conhecida, mas não provida” (TRF2, Apelação Cível 2001.02.01.040357-7, rel. Abel Gomes, DJ 15-1-2010).

“*Propriedade industrial*. Ação de obrigação de fazer com preceito cominatório visando impor à ré a abstenção de utilização de domínio na Internet. Impossibilidade. Comprovação de registro da marca pela requerente que apesar de não lhe atribuir exclusividade, confere-lhe o direito de uso do domínio na Internet. Inocorrência de nulidade da sentença em razão do julgamento antecipado da lide. Improcedência da ação principal e da medida cautelar confirmada. Sentença mantida. Recurso não provido” (TJSP, Apelação 0035429-24.2006.8.26.0000, rel. Des. Luís Francisco Aguilar Cortez, j. 29-11-2011).

“Apelação. Direito Empresarial. Domínio na Internet. Cancelamento e abstenção de uso. Nome de domínio que coincide com a marca objeto do depósito, pela autora, de pedido de registro no INPI. Acesso ao sítio que automaticamente direciona o internauta à página destinada aos produtos da corré, similares àquele oferecido pela autora e destinados ao mesmo público-alvo. Concorrência desleal caracterizada. Necessidade de cancelamento do registro. Dano moral à pessoa jurídica, embora possível, não caracterizado no caso concreto. Apelo a que se dá parcial provimento” (TJSP, Apelação 0009528-39.2009.8.26.0068, rel. Des. Pereira Calças, j. 8-11-2011).

“*Propriedade industrial*. Ação de abstenção de atos de concorrência desleal, objetivando sejam as rés obstadas a usar os nomes de domínio www.webmotos.com.br e www.webmotos.com. Alegação de concorrência desleal. Reforma da sentença que se impõe. Existência de similitude de atividades empresariais das partes. Autora que registrou seu nome precedentemente perante o INPI. Descabimento, entretanto, do pleito indenizatório. Apelo parcialmente provido” (TJSP, Apelação 9134892-72.2009.8.26.0000, rel. Des. Sebastião Carlos Garcia, j. 8-11-2011).

“*Prestação de serviços de 'Internet'. 'Google ad words'. 'Link' patrocinado. Pessoa jurídica. Serviço contratado para incrementar negócios. Usuário que era redirecionado para o 'site' de concorrentes. Falha na prestação do serviço. Risco do negócio. Fortuito interno. Dano moral adequadamente arbitrado. Dano material não comprovado. Sú-*

mula 227 do STJ. A prova dos autos não deixa dúvidas quanto ao defeito do serviço ‘ad words’ oferecido pela ré, frustrando as expectativas da autora, ora contratante, que pretendia incrementar suas atividades empresariais. Apurou-se que quando o usuário da ‘Internet’ acessava o ‘site’ do ‘Google’ e pesquisava pelo nome da autora, no espaço reservado para os *links* patrocinados, embora aparecesse o ‘site’ da autora, os usuários eram encaminhados para o ‘site’ de seus maiores concorrentes. Argumenta o réu em sua defesa que os alegados danos foram causados por terceiros concorrentes da autora, cuja conduta — uso indevido de marca — não poderia ser por ela evitada. Afirmou, no mais, que não existe tecnologia capaz de impedir que determinadas palavras-chaves sejam utilizadas por terceiros, especialmente porque não tem como aferir quem é concorrente de quem e quais marcas ou expressões estão protegidos. No entanto, tais teses defensivas não podem ser opostas contra a autora porque configurado está o fato do serviço, inserindo-se a situação retratada nos autos em típico risco do negócio. Desse modo, não se exime a responsabilização civil e consumerista do réu, porquanto se trata de fortuito interno, ou seja, risco que se insere na atividade normalmente desenvolvida pelo réu. A pessoa jurídica é passível de lesão em sua honra objetiva, compreendendo esta, como ofensa à imagem, ao seu bom nome, diminuição do conceito público de que goza na sociedade. Nesse sentido, a Súmula 227 do STJ: ‘A pessoa jurídica pode sofrer dano moral’. *In casu*, pode-se entender que o serviço contratado operou-se de forma contrária ao que foi ajustado, ou seja, ao invés de atrair a clientela, houve um desvio da clientela. Desprovimento dos recursos” (TJRJ, Apelação 0003615-70.2008.8.19.0209, rel. Des. Roberto de Abreu e Silva, j. 20-7-2011).

FRAUDES ELETRÔNICAS — RESPONSABILIDADE CIVIL

Comentários:

As fraudes praticadas pela rede mundial de computadores estão crescendo vertiginosamente e, por incrível que pareça, a dificuldade da imputação de sua autoria permanece. Daí a importância da prevenção e guarda adequada de *logs* quer pelos provedores de acesso, quer pelas instituições financeiras, considerando o crescente aumento do uso da Internet para operações financeiras.

Nos últimos anos o Judiciário brasileiro passou a entender que há responsabilidade do usuário de Internet *Banking* no sentido de dever de cumprir com as recomendações de segurança fornecidas pelo Banco. E, quando não as segue, não há que se falar em hipossuficiência, nem tampouco ressarcimento. Por isso os Bancos passaram a fazer campanha maciça de comportamento seguro com foco nos clientes, até para conseguir provar juridicamente que houve culpa do mesmo no uso do recurso facilitando a ocorrência da fraude.

Há dever de segurança de ambas as partes. A Sociedade Digital não tem mais fronteira física, mas o Banco responde pelo que está no Servidor, e o Usuário responde pelo uso de um equipamento seguro, por se conectar e navegar de forma protegida.

“Ação de indenização por danos materiais e morais. Empréstimo via Internet. Contratação fraudulenta. Descontos indevidos em conta corrente. Culpa exclusiva da vítima. Não configuração. Exclusão da responsabilidade da instituição financeira por culpa de terceiro. Impossibilidade. Restituição dos valores pagos indevidamente. Direito reconhecido. Repetição em dobro do indébito. Ausência de má-fé. Não cabimento. Dano moral configurado. Valor indenizatório excessivo. Redução. Restando inteiramente comprovado que a contratação do empréstimo junto à instituição financeira apelante foi realizada mediante fraude praticada por terceiro, sem a participação da correntista e nem tendo ela contribuído de qualquer forma para o evento danoso, há que se reconhecer a ilegitimidade da contratação, a total irregularidade e ilicitude dos descontos efetuados em sua conta corrente e o consequente direito da mesma à restituição dos valores pagos indevidamente. Contudo, não existindo sequer indícios de que tenha a instituição financeira agido de má-fé em relação a tal contratação, não se faz cabível a dobra prevista no art. 42 do CDC, devendo os valores pagos pela apelada serem-lhe restituídos de forma simples. Pelas mesmas razões ora descritas, tem-se que restou configurado o dano moral suportado pela correntista apelada, dano que inclusive é presumido e decorre dos próprios des-

contos injustos, não sendo afastados pela suposta culpa exclusiva da vítima, no caso não comprovada, muito menos de terceiro. A indenização deve ser fixada segundo critérios de razoabilidade e proporcionalidade e com observância das peculiaridades do caso, que na hipótese apontam para a necessidade de redução do valor estabelecido na Instância *a quo*, inclusive para não dar ensejo ao enriquecimento ilícito da consumidora apelada e, ainda, para melhor se amoldar aos valores normalmente adotados por este Tribunal” (TJMG, Recurso Cível 0257000-87.2007.8.13.0487, rel. Arnaldo Maciel, j. 24-8-2010).

“Relação de Consumo. Ação com pedido indenizatório por danos materiais e morais. Fraude eletrônica praticada via Internet. Evidente falha de serviço do réu ao autorizar a transferência de valores da conta corrente da autora, que sequer havia saldo disponível para realizar tal transação. Responsabilidade objetiva do réu, na forma do Código de Defesa do Consumidor. Descuido da segurança no seu atuar, ocasionando prejuízos financeiros à autora. O réu não logrou êxito em comprovar qualquer excludente de sua responsabilidade. Dano moral reconhecido cabível de indenização. Evidente o nexo de causalidade e o dano sofrido pela autora. Quanto ao valor fixado para a indenização, deve o julgador ater-se em critérios de razoabilidade e proporcionalidade, bem como o caráter pedagógico da medida. Recurso a que se nega seguimento, na forma autorizada pelo art. 557 do Código de Processo Civil” (TJRJ, 0150855-76.2006.8.19.0001, 15ª Câmara Cível, rel. Cláudio Brandão, DJ 20-8-2010).

*“(…) Não há evidências de que houve falha no sistema disponibilizado pelo réu. Ao contrário, o conjunto de medidas de segurança simultâneas adotadas pelo réu no âmbito virtual, tais como exigência de cartão magnético, senha do cartão, senha eletrônica da Internet e cartão de segurança, afim de que o usuário possa realizar operações via Internet, revelam um sistema de segurança eficaz. Sem mencionar ainda, as informações e alertas constantes no *site* do banco acerca das possíveis fraudes e como evitá-las (...) A sentença que reconheceu a culpa exclusiva da vítima no uso do Internet *Banking* e isentou o banco de culpa, foi mantida pelo Tribunal” (TJSP, Apelação 990.10.106412-0, rel. Des. Tersio J. Negrato, j. 28-4-2010).*

“Apelação Cível. Ação de indenização. Conta bancária. Invasão por terceiro através da rede mundial de computadores. Falha no sistema. Relação de consumo. Inteligência do art. 14 do Código de Defesa do Consumidor. Não

demonstração da culpa exclusiva da vítima. Inscrição indevida. Dever de indenizar. Danos materiais e morais. Impugnação genérica. Manutenção. Sentença escoreita. Recurso desprovido. 1. Impossibilitado ao banco repassar os riscos das operações realizadas através da Internet ao correntista, em especial os prejuízos causados pela ação criminosa de *hackers*, cabendo-lhe responder, objetivamente, pelos danos sofridos pelo cliente ante a deficiência nos serviços disponibilizados. 2. O valor da indenização por danos materiais corresponde ao desfalque patrimonial sofrido e não impugnado. 3. A indenização arbitrada a título de danos morais, ante a inscrição injusta motivada por dívidas não autorizadas, foi fixada em valor aquém do arbitrado por esta Câmara em situações similares, de modo que, sua redução, sem motivo relevante, implicaria em cifra irrisória que nada compensaria o ofendido, tornando o dano insignificante, premiando o ofensor, sem cumprir seu papel punitivo-educativo de futuros desvios" (TJPR, Apelação Cível 0608520-1, rel. Hélio Henrique Lopes Fernandes Lima, j. 10-6-2010).

"Indenização por danos morais. Instituição financeira. Pagamentos e concessão de empréstimo realizados por terceiros via sistema eletrônico Internet. Responsabilidade objetiva. Dano moral configurado dever de indenizar. Procedência do pedido. Confirmação da sentença. A responsabilidade do prestador, pela falha do serviço, nas relações de consumo, é de natureza objetiva, nos termos do art. 14 do Código de Defesa do Consumidor. Restando comprovado que a conta corrente do autor foi movimentada por terceiros em razão de fraude praticada via Internet, é certo que a responsabilidade pelo débito gerado deve ser imputada à empresa que disponibilizou o sistema de movimentação eletrônica. A instituição financeira não se exime da responsabilidade alegando que a fraude se deu por culpa exclusiva do autor, eis que cabe a ela, que optou por disponibilizar movimentações eletrônicas via Internet, adotar sistemas eletrônicos seguros e capazes de impedir a ação de fraudadores. Configura-se dano moral a angústia do autor em constatar operações promovidas em sua conta por terceiros" (TJMG, Recurso Cível 1.0024.06.128847-8/001(1), rel. José Affonso da Costa Côrtes, j. 13-5-2010).

"Processual penal. Furto mediante fraude. Compra com cartão de débito. Local de consumação do delito. 1. É pacífico que os crimes de saques sem o consentimento da vítima, por meio de clonagem de cartão de crédito ou fraude eletrônica via Internet configuram a conduta tipificada no art. 155, § 4º, II, do CP, tendo em vista a utilização da fraude como meio de burlar a vigilância da vítima e subtrair o bem sem o seu consentimento. 2. A consumação do delito furto mediante fraude ocorre no

lugar onde se localiza a agência do correntista, pois a inversão da posse acontece quando o bem sai da esfera de disponibilidade da vítima, gerando prejuízo. 3. Conflito conhecido para declarar a competência da Vara Federal de Itaboraí para o processamento do feito" (TRF2, Conflito de Jurisdição 2010.02.01.002399-0, rel. Liliane Roriz, DJ 4-5-2010).

"Ação de indenização. Instituição financeira. Fraude. Operações bancárias via Internet. Relação de consumo. Falha na prestação do serviço. Danos morais. Configuração. Quantum. A responsabilidade do fornecedor, em decorrência de falha na prestação do serviço, é objetiva, nos exatos termos do art. 14 do CDC, bem como do art. 927, parágrafo único, do CC/2002. Nestes casos não se configura a excludente de ilicitude denominada fato de terceiro, uma vez que, não obstante a ação fraudulenta possa até ser considerada inevitável, não era ela imprevisível, visto que a instituição financeira tem conhecimento dos riscos das transações financeiras realizadas através da rede mundial de computadores, e, ainda assim, os assume ao oferecer esta forma de serviço aos seus clientes. É impossível ignorar a aflição, o desespero e os transtornos decorrentes do sumiço de considerável quantia da conta corrente do consumidor, de sorte estar comprovado o dano moral em face das dificuldades financeiras e do receio de sofrer significativa lesão no patrimônio. O valor da reparação não deve constituir enriquecimento sem causa, mas deverá ser desestímulo à repetição da conduta danosa" (TJMG, Recurso Cível 5210061-49.2009.8.13.0145, rel. Nicolau Masselli, j. 29-4-2010).

"Penal. Processual penal. Prova indiciária robusta e não contraditada. Condenação. Possibilidade. Furto qualificado (fraude). Art. 155, § 4º, II, do CP. Transferência bancária fraudulenta via Internet. 1. Tendo sido a denúncia oferecida com base em indícios veementes do cometimento do delito, é indispensável que o acusado apresente contraindícios ou provas favoráveis à sua versão dos fatos, a fim de que se tenha respaldo a um decreto absolutório. 2. Não tendo havido comprovação quanto à tese defensiva, deixando o acusado, pois, de observar o disposto no art. 156 do CPP, merece reforma a sentença absolutória, restando condenado o réu, porquanto responde pelo delito de furto qualificado pela fraude (art. 155, § 4º, II, do CP) aquele que, sem autorização do titular da conta corrente, realiza transferências de valores depositados em agência bancária, por meio da Internet" (TRF4, Apelação Criminal 2006.71.10.001399-0, rel. Tadaaki Hirose, DJ 27-4-2010).

“Acordam os desembargadores integrantes da décima câmara cível do tribunal de justiça do Estado do Paraná, por unanimidade de votos, em negar provimento ao recurso, e conhecer em parte do recurso adesivo e, na parte conhecida, dar parcial provimento ao recurso. Ementa: Apelação cível. Ação de indenização por danos materiais e morais. Movimentação de conta bancária por “hackers”, via internet. Contratação de empréstimo e transferência de numerário. Responsabilidade objetiva da instituição financeira. Atividade de risco. Falha na prestação de serviço configurada. Excludentes de responsabilidade. Inocorrência. Culpa exclusiva da vítima não demonstrada. Danos materiais. Pleito de devolução em dobro dos valores. Inovação recursal. Restituição do valor da transferência. Omissão da sentença complementação devida. Efeito devolutivo. Sucumbência recíproca. Distribuição mantida. Honorários advocatícios. Quantum adequado. Recurso de apelação desprovido. Recurso adesivo conhecido em parte e, na parte conhecida, parcialmente provido. 1 — Restando incontroverso que os valores foram retirados da conta corrente do autor, através da Internet, por “hackers”, mediante a utilização de meios fraudulentos, deve o banco restituir ao correntista os valores indevidamente contratados e transferidos daquela conta. A responsabilidade do fornecedor do serviço é objetiva, por envolver uma atividade de risco, nos termos do art. 927, parágrafo único, do Código Civil, e conforme disposição do art. 14 do Código de Defesa do Consumidor, somente se eximindo o fornecedor de qualquer obrigação, caso comprove que tendo prestado o serviço, o defeito inexiste; a culpa exclusiva do consumidor ou de terceiro (art. 14, § 3º, I e II, do CDC), ou ainda, que o evento decorreu de caso fortuito ou força maior, ônus do qual não se desincumbiu o requerido. 2 — Não se conhece do recurso, no tocante ao pedido de devolução em dobro dos valores, vez que não foi objeto de discussão na causa, sendo levantada somente por ocasião do recurso de apelação, configurando evidente inovação de tese na fase recursal. 3 — O Tribunal está autorizado a decidir todas as questões relativas à demanda, ainda quando a sentença não as tenha julgado por inteiro (art. 515, § 1º, do CPC), no caso, impõe condenar a requerida a restituir, também, o numerário transferido indevidamente para outra conta bancária, com o desconto da quantia restituída pela instituição financeira. 4 — Considerando que o autor decaiu no pleito de indenização por danos morais, a sucumbência deverá ser recíproca e proporcionalmente distribuída e compensada entre as partes, na forma do art. 21 do Código de Processo Civil. Ademais, tendo em vista o que foi pedido e o que foi deferido, deve ser mantida a distribuição constante na sentença. 5 — Tendo em vista o grau de zelo profissional, o lugar da prestação, a natureza e importância da causa, o trabalho realizado e o tempo despendido, não se mostram excessivos os honorários fixados na sentença” (TJPR, 10ª Câmara Cível, Apelação Cível 0551842-7, rel. Luiz Lopes, j. 22-4-2010).

“Apelação Cível. Interposição tempestiva. Ação de indenização. Conta bancária. Invasão por terceiro através da rede mundial de computadores. Falha no sistema. Relação de consumo. Inteligência do art. 14 do Código de Defesa do Consumidor. Não demonstração da culpa exclusiva da vítima. Dever de indenizar. Dano moral. Dispensa de prova. Valor indenizatório. Adequação e proporcionalidade. Sentença correta. Recurso desprovido. 1. Tempestivo o recurso apresentado dentro do lapso quinzenal aludido no art. 508 do CPC e em observância a regra de cômputo dos prazos processuais (art. 184 do CPC). 2. Impossibilitado ao banco repassar os riscos das operações realizadas através da ‘Internet’ ao correntista, em especial, os prejuízos causados pela ação criminosa de ‘hackers’, cabendo-lhe responder, objetivamente, pelos danos sofridos pelo cliente ante a deficiência nos serviços disponibilizados. 3. A prova do dano moral deriva do próprio fato ofensivo, no caso, a má prestação do serviço. Apelação Cível n. 631.298-5 4. O valor fixado a título de indenização por danos morais é proporcional a gravidade da ofensa, as circunstâncias do caso, a situação econômica das partes, servindo de meio hábil para, se não evitar, ao menos coibir, episódios como aqui relatado” (TJPR, Apelação Cível 0631298-5, rel. Hélio Henrique Lopes Fernandes Lima, j. 25-3-2010).

“Responsabilidade civil. Débitos efetuados em conta corrente do autor, movimentação mediante serviço disponibilizado pelo banco via Internet. Fraude. Dever do banco de indenizar. Agravo regimental a que se nega provimento” (STJ, AgRg no Ag 940.608/RJ, rel. Ministro Luis Felipe Salomão, j. 4-3-2010).

“Processo penal. Transferência fraudulenta de valores pela Internet. Tipificação. Crime de furto qualificado mediante fraude. Correntista da caixa econômica federal. Competência da Justiça Federal. Art. 109, IV, da Constituição da República. 1. Compete à Justiça Federal processar e julgar o delito de furto qualificado mediante fraude (art. 155, § 4º, II, do Código Penal) perpetrado contra correntista da Caixa Econômica Federal, pois o delito atinge o patrimônio dessa empresa pública federal, na medida em que estaria obrigada a ressarcir o correntista do prejuízo causado pelo delito e tendo em vista que o crime sempre há de causar abalo na credibilidade de seus serviços, ocasionando, portanto, diversos prejuízos à instituição, o que reclama a aplicação do art. 109, IV, da Constituição da República. 2. Recurso em sentido estrito provido” (TRF3, Recurso em Sentido Estrito 2009.61.02.011780-6, rel. André Nekatschalow, DJ 8-3-2010).

“Ação de indenização. Movimentação bancária por terceiros via Internet. Responsabilidade da instituição financeira pelos danos advindos da fraude. Dano moral

configurado. Valor da indenização. A apreensão e insegurança suportados pelo cliente bancário em razão de operações financeiras fraudulentas realizadas por terceiros, via Internet, podem configurar danos morais indenizáveis. A instituição financeira deve ser responsabilizada pelos prejuízos morais causados ao cliente pela falha do serviço, especialmente por ter demonstrado desinteresse na solução do evento. Na fixação da indenização pelos danos morais, deve-se atentar para as circunstâncias dos fatos e das partes, evitando o enriquecimento indevido, mas proporcionando à vítima uma satisfação e ao ofensor um desestímulo à prática de condutas abusivas” (TJMG, Recurso Cível 0090442-72.2007.8.13.0440, rel. Tiago Pinto, j. 25-2-2010).

“Penal e processual penal. Transação bancária fraudulenta. Tipificação. Consumação. Competência. I — As transações bancárias fraudulentas realizadas mediante a utilização de cartão clonado ou por meio de fraude eletrônica via Internet configuram a prática do crime de furto mediante fraude, uma vez que a fraude é utilizada para burlar a esfera de vigilância da vítima. II — O processo e julgamento do delito é da competência do juízo com jurisdição do local de consumação do crime que, no caso, consuma-se no momento em que a coisa é retirada da esfera de disponibilidade da vítima, sem o seu consentimento, ou seja, o local onde o correntista mantém a conta bancária fraudada. III — Entendimento assentado pelo Colendo Superior Tribunal de Justiça e precedentes dos Tribunais Regionais Federais. IV — Conflito de competência improcedente” (TRF3, Conflito de Jurisdição 2009.03.00.042649-1, rel. Henrique Herkenhoff, DJ 4-2-2010).

“Apelação. Repetição de matéria versada na contestação. Impugnação específica da decisão. Observância da motivação recursal. Relação de consumo. Inexistência de falha na segurança. Culpa exclusiva do consumidor ou de terceiro. Excludentes de responsabilidade. Ônus da prova do fornecedor. Fraude em meio eletrônico. Subsistência da responsabilidade do fornecedor. Contribuição para o resultado com o fornecimento do serviço suscetível a falhas. 1 — A devolução da matéria apresentada em sede de contestação não constitui violação ao princípio da motivação recursal, desde que a matéria seja apresentada através de impugnação específica da sentença. 2 — A inexistência de falha na segurança de serviço prestado ou a culpa exclusiva de terceiro ou do consumidor consistem em excludentes de responsabilidade cuja comprovação deve ser implementada pelo fornecedor, sob pena de responder pelos danos ocasionados ao consumidor. 3 — A fraude realizada por terceiro em meio eletrônico não exime a responsabilidade do fornecedor que

contribui com o resultado na medida em que ofertou serviço suscetível de falha na segurança” (TJMG, Recurso Cível 0172561-03.2008.8.13.0878, rel. Pedro Bernardes, j. 2-2-2010).

“Reparação de danos materiais e morais. Transferência de valores e pagamento de DOC. Bancário via Internet. Alegação de fraude. Imputação da autoria da operação à correntista. Ausência de prova nesse sentido. Demonstração que incumbia ao banco. Danos morais configurados, na hipótese concreta. Ao imputar à demandante a responsabilização pelas operações bancárias realizadas via Internet, era do banco, sem dúvida, o encargo de produzir prova cabal nesse sentido, não só por se tratar de relação de consumo, sendo o fornecedor o único detentor de tais dados, mas notadamente porque da parte autora não se pode exigir a produção de prova negativa. Danos morais configurados, no caso concreto, ante a negativa de restituição dos valores, com privação de capital significativo por mais de cinco meses e, especialmente, em razão do constrangimento decorrente da injusta acusação do banco no sentido de que a autora teria contribuído para a efetivação da fraude, ao repassar dados a terceiros não autorizados. Atendimento, também, da função dissuasória da responsabilidade civil. Recurso desprovido” (TJRS, Recurso Cível 71002243293, rel. Eugênio Facchini Neto, j. 28-1-2010).

“Competência. Saque fraudulento de conta corrente. Juízo da agência responsável pela conta. 1. Na hipótese de ocorrer saque ou transferência de valores mediante ilegítimo emprego da Internet ou cartão clonado, a competência é determinada em função do local da agência responsável pela administração da conta debitada. Precedentes do STJ. 2. Conflito de competência improcedente” (TRF3, Conflito de Jurisdição 2009.03.00.025641-0, rel. André Nekatschalow, publ. 3-12-2009).

“Penal e processo penal. Apelação criminal. Furto de valores de conta corrente mediante fraude. Transferência de valores via Internet. Materialidade e autoria. Comprovação. Pena-base. Redução. Circunstâncias do crime desfavoráveis. Valor do dia-multa. Ausência de fundamentação. Fixação do mínimo legal. Parcial provimento do recurso. I — Conduta consistente na transferência de valores de correntistas da Caixa Econômica Federal, utilizando contas de amigos e parentes como de passagem dos valores que eram subtraídos de outras contas correntes por meio de fraude, vindo, a CEF, a indenizar os titulares das contas que eram esvaziadas. Provas documentais e orais nesse sentido. II — Tipificação da condu-

ta no art. 155, § 4º, II, do Código Penal, uma vez que houve o emprego de meios ardilosos ou insidiosos para burlar a vigilância dos lesados. No estelionato, é a vítima quem entrega a coisa por causa da fraude. No furto mediante fraude, esta acarreta o acesso à coisa subtraída, desviando a atenção do sujeito passivo. Correta a *emendatio libelli* implementada na sentença. III — O valor de R\$ 15.000,00 não é de tamanha monta a ensejar o aumento da pena-base pelas graves consequências do crime, mormente considerando que se chegou a tal valor através de uma conduta continuada. Redução da pena-base. IV — O crime praticado via Internet em muito dificulta o rastreamento da fraude perpetrada e acarreta sempre maior necessidade de cuidados com a segurança das operações realizadas *online*. Circunstâncias do crime desfavoráveis. Pena-base fixada um pouco acima do mínimo legal. V — O aumento do valor do dia-multa precisa ser fundamentado em situação econômica favorável. Com a inexistência de fundamentos concretos, o dia-multa deve ser fixado no mínimo legal. VI — Recurso parcialmente provido” (TRF2, Apelação Criminal 2004.51.01.530918-9, rel. Abel Gomes, publ. 29-7-2009).

“Ação de indenização. Fraude em conta corrente. Responsabilidade pela segurança das operações eletrônicas. Cadastro de inadimplentes. Inscrição indevida. Danos morais. Critérios de fixação. Caráter punitivo e compensatório. Prestação pecuniária à instituição de caridade. Ausência de permissivo legal. Exclusão. Voto vencido. A instituição financeira é responsável pela segurança das operações eletrônicas disponibilizadas ao correntista, não sendo aceitável a transferência do risco da atividade para o consumidor, visto ser prática vedada pelo art. 51, I, IV e XV, do Código de Defesa do Consumidor. Aquele que tem o nome inscrito no cadastro de inadimplentes em razão da negligência da instituição financeira em garantir a segurança das operações bancária, sofre danos morais indenizáveis. A dosagem da indenização por danos morais obedece ao critério do arbitramento judicial, norteado pelos princípios da proporcionalidade e da razoabilidade, observando-se o caráter compensatório para a vítima e punitivo para o ofensor. Inexiste permissivo legal para que a parte condenada ao pagamento de indenização civil seja obrigada a arcar com prestação pecuniária em favor de instituição de caridade estranha à demanda. Primeiro e segundo recursos providos em parte. V.V.: Deve ser mantida a indenização concedida na Primeira instância. (Des. Gutemberg da Mota e Silva)” (TJMG, Recurso Cível 2126445-48.2008.8.13.0701, rel. Marcos Lincoln, j. 14-7-2009).

“Ação de indenização. Anulatória de débito. Transações bancárias via Internet. Incerteza quanto à autoria. Responsabilidade do banco. Dano moral. Existente. Danos

materiais. Devidos. Ao disponibilizar a realização de transações bancárias pela Internet, prometendo segurança, responsabiliza-se civilmente a instituição financeira pelos prejuízos sofridos por correntistas que tiverem suas contas invadidas por ‘hackers’. Havendo falha na prestação do serviço, por negligência da empresa (instituição bancária), acarretando prejuízos ao consumidor, constitui ônus processual do fornecedor provar a não existência do alegado defeito. O valor do dano moral deve ser arbitrado com moderação, norteando-se o julgador pelos critérios da gravidade e repercussão da ofensa, da posição social do ofendido e da situação econômica do ofensor” (TJMG, Apelação Cível 1.0183.07.122914-4, rel. Des. Antônio de Pádua, publ. 10-3-2009).

“Ação de indenização por danos morais e materiais. Movimentação bancária por terceiros via internet. Responsabilidade da instituição financeira pelos danos advindos da fraude. Danos morais. Indenização devida. I. Se o banco oferece serviços de acesso à conta corrente e movimentações financeiras via Internet, deve garantir a segurança do sistema. Se este é falho, permitindo que terceiros tenham acesso às contas dos clientes e façam operações de crédito, saque e transferências, o banco deve assumir a obrigação de reparar os danos que possam decorrer do defeito na prestação do serviço. II. A privação do cliente do dinheiro que havia em sua conta e seria usado para suas necessidades por si só configura dano moral, passível de reparação” (TJMG, Apelação cível 1.0701.07.185927-9/001, rel. Des. Generoso Filho, DOJ 8-9-2008).

“Consumidor. Contrato de conta corrente. Saques via Internet realizados por terceiros. Falha de segurança comprovada. Responsabilidade civil. Danos morais ocorrentes. 1. A alegação do autor de que não teria efetuado compra ou pagamento via Internet é plausível. De conhecimento notório que os sistemas operacionais dos bancos envolvendo negociações *online* são passíveis de fraude. Inclusive comprova o autor às fls. 18/19 que não foi feito por seu perfil de usuário o pagamento de contas via Internet, ainda mais no valor da negociação aqui reclamada. Nesse passo, possível a distribuição dinâmica do ônus da prova. (...) 3. De outro lado, cingiu-se o réu a alegar a absoluta segurança de seu sistema, referindo serem necessários senhas e cartões para que, conjuntamente utilizados, sejam possíveis as negociações. No entanto, não provou ter o autor solicitado ou recebido as referidas senhas, tampouco que este costumeiramente faria uso de tais serviços. Além disso, possível seria ao réu demonstrar alguma relação entre o recebedor do pagamento e o autor, o que também não foi feito. 4. Assim, não tendo comprovado a responsabilidade do autor pelos débitos em sua conta corrente, surge para o banco réu o dever de

indenizar. 5. Dano moral configurado, já que comprovado que os transtornos sofridos extrapolaram os meros dissabores da vida. O valor do desfalque na conta corrente do autor tornou seu saldo negativo, acarretando danos morais indenizáveis. O valor fixado na sentença a título de indenização por danos morais (R\$ 3.000,00), por observar os postulados da proporcionalidade e da razoabilidade, não merece ser reduzido. Sentença confirmada por seus próprios fundamentos. Recurso improvido" (TJRS, Recurso Cível 71001629682, rel. Des. Ricardo Torres Hermann, j. 19-6-2008).

"Direito privado não especificado. Fraude eletrônica, via Internet. Prestação de serviços defeituosa, que permite ocorrência de fraude, enseja dever de indenizar. O serviço prestado pelo banco apresentou-se defeituoso, tanto que permitiu que terceiro de má-fé acessasse a página pessoal do banco, ainda que via PC do autor e manipulasse dados e senha, debitando indevidamente valores na conta do autor. Colocando o banco à disposição de seus clientes a possibilidade de movimentar as contas e realizar operações financeiras via Internet, deve criar mecanismos que impeçam a ocorrência de fraudes e, quando os mecanismos de segurança falham, responde o banco, objetivamente, pelos danos que advierem a seus correntistas. Recurso improvido" (TJRS, Recurso Cível 71001437136, rel. Angela Maria Silveira, j. 31-1-2008).

"Embargos infringentes. Direito do consumidor. Saques com cartão magnético não reconhecidos pelo correntista. Inversão do ônus da prova. Dever do fornecedor de garantir a segurança do consumidor. Provimento do recurso. Uma vez invertido o ônus da prova, por força de decisão preclusa, não cabe exigir do consumidor a prova da falha da instituição bancária em permitir a realização de saques que o autor impugna — antes, sobre o fornecedor é que pende o ônus de comprovar a culpa do consumidor no evento. oferecimento de facilidades eletrônicas para as transações financeiras, embora sejam também do interesse do consumidor, atendem sobretudo às expectativas de ganhos das instituições financeiras, que com isto, poupam considerável montante, por exemplo, de pagamento de funcionários. Se o fornecedor lucra com o sistema por ele implantado, deve também responder pelos prejuízos advindos de suas lacunas — *ubi emulumentum, ibi onus*. Por outro lado, a prática corriqueira de fraudes em *sites* de instituições financeiras, clonagem de cartões, subtração de dados pessoais (inclusive senhas) é de tal maneira conhecida e divulgada que não se pode deixar de considerar verossímeis as alegações do autor, à luz das regras ordinárias de experiência — sendo certo que, entre os direitos básicos do consumidor, está o de ter garantida sua segurança na utilização dos serviços e produtos postos no mercado. Provimento do recurso" (TJRJ, Bem. Infr. 2008.00500038, rel. Marcos Alcino A. Torres, j. 25-3-2008).

"Serviço bancário. Internet. Transferência de valores não autorizada pela titular. Relação de consumo. Inversão do onus probandi. Contrato de depósito. Dever de ressarcir os valores depositados. Fraude. Fortuito interno. Dano moral não configurado. Restou incontroverso nos autos as transferências *online* efetuadas na conta corrente da autora. Malgrado o réu afirmar que possui rígido esquema de segurança para operações realizadas via Internet, o que se infere dos autos é que o mesmo não funcionou. Demais, tal fato só se comprovaria através de perícia a qual não foi requerida pelo réu. Assim, o réu não se desincumbiu do *onus probandi* trazendo para si a responsabilidade pelos danos causados à autora. A prova dos autos evidencia a ação de terceiros fraudadores (*hackers*), situação que não exime a responsabilização civil do réu, porquanto se trata de fortuito interno. Há que se reconhecer a falha na prestação de serviços sendo corolário, a responsabilidade civil objetiva do réu fundada no art. 14, *caput*, e § 1º, II, da Lei n. 8.078/90 e na teoria do risco empresarial, considerando que quem retira proveito de uma atividade de risco, com probabilidade de danos, obtendo vantagens, lucros, benefícios, deve arcar com os prejuízos perpetrados. O descumprimento contratual constitui fonte de obrigação proveniente de ilícito relativo e de consumo, cuja sanção consiste em perdas e danos. Daí se conclui que não houve dano extrapatrimonial a ensejar a reparação, merecendo reforma o r. *decisum* nesse ponto. Dar parcial provimento ao recurso. Art. 557, § 1º-A do CPC" (TJRJ, Bem. Infr. 2008.00500038, rel. Des. Roberto de Abreu e Silva, j. 18-2-2009).

"Ação de reparação de danos. Cartão de crédito. Vendas. Loja virtual. CDC. Compra contestada. Rede. Ambiente seguro. Estorno de valores. 1. Deve ser considerada consumidora a microempresa praticante de atos de comércio via Internet, que aliena os seus produtos em razão de convênio firmado com administradora de cartão de crédito, a qual, como fornecedora, obtém do comprador o número do cartão de crédito e demais dados inerentes à aprovação do crédito, atraindo para si a avaliação do risco, aprovando ou não a operação de venda. 2. O estabelecimento comercial que realiza suas vendas pela Internet, mediante a utilização de sistema fornecido e gerenciado por determinada rede, a qual, além de garantir a existência de uma operação segura, é a única responsável pela avaliação e aprovação da operação mercantil a ser consumada, não pode ser penalizado por fraudes que o próprio sistema não conseguiu evitar, mesmo porque a loja virtual, consoante comum conhecimento, não tem qualquer contato com o cartão utilizado, tampouco com o seu titular ou portador. (TJMG, Apelação cível 1.0024.06.996622-4/001, rel. Des. Guilherme Luciano Baeta Nunes, *DOJ* 17-5-2007).

"Conflito negativo de competência. Penal e processo penal. Fraude eletrônica na Internet. Transferência de valores de conta corrente da caixa econômica federal. Crime

de furto mediante fraude. Consumação no local de subtração do bem. Aplicação do art. 70 do CPP. 1. A subtração de valores de conta corrente, mediante transferência fraudulenta para conta de terceiro, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, II, do Código Penal. Precedentes da Terceira Seção. 2. É competente o Juízo do lugar da consumação do delito de furto, local onde o bem é subtraído da vítima. 3. Conflito conhecido para declarar a competência do suscitante, Juízo Federal da 2ª Vara Criminal da Seção Judiciária do Estado do Espírito Santo” (STJ, CC 81.477/ES, rel. Ministro Og Fernandes, j. 27-8-2008).

“Habeas corpus. Prisão preventiva. Art. 288, 171 c/c 71, CPB. Materialidade e indícios suficientes de autoria. Gravidade dos fatos. Organização e estruturação do bando. Forma de atuação. Clonagem de cartões de crédito. Compra de passagens via Internet. Vultoso prejuízo a administradoras dos cartões e companhias aéreas. Decisão suficientemente fundamentada. Denúncia. Satisfação dos requisitos previstos nos arts. 41 e 43 do CPP. Exclusão de tipo penal por inépcia. Determinação de remessa dos autos ao Ministério Público para os fins do art. 89 da Lei n. 9.099/95. Impossibilidade. Constrangimento ilegal inexistente. 1. Nenhum constrangimento ilegal pode ser extraído da decisão que para decretar prisão preventiva, reporta-se, concreta e suficientemente, à gravidade dos fatos (quadrilha formada para o fim de prática de estelionatos, estes em continuidade delitiva), à organização e estruturação da quadrilha, à forma de atuação, ao prejuízo sofrido por administradoras de cartão de crédito e companhias aéreas, sendo pacífico que primariedade e bons antecedentes, residência fixa e profissão definida não excluem possibilidade de prisão cautelar se os fatos a justificam, pacífico em doutrina e em jurisprudência que tal não ofende o princípio constitucional da presunção de inocência. 2. A via estreita do *habeas corpus* não comporta dilação probatória. Se a denúncia obedece aos requisitos dos arts. 41 e 43 do CPP, não há que se falar em possibilidade de reconhecimento de sua inépcia para, excluindo discussão relativa a tipo penal, determinar-se remessa dos autos ao Ministério Público para oferecimento de proposta relativa ao art. 89 da Lei n. 9.099/95.3. Ordem denegada” (TJDF, HC 20090020003022, rel. Maria Ivatônia, DJ 11-3-2009).

“Ação de indenização por danos materiais e morais. Autora que fundamenta a pretensão em operações realizadas indevidamente em sua conta corrente. Instituição financeira que não produziu provas aptas a demonstrar que as movimentações foram efetuadas pela correntista. Inteligência dos arts. 6º, V, e 14, § 3º, do Código de Defesa do Consumidor. Ato que acarreta a presunção dos prejuízos sofridos pela autora. Dever de indenizar é de rigor. Dano moral caracterizado. Manutenção da decisão. Negado provimento ao recurso” (TJSP, Apelação 0123424-98.2008.8.26.0002, rel. Des. Ligia Araújo Bisogni, j. 23-11-2011).

“Responsabilidade civil. Indenização. Danos morais. Empréstimo contraído por terceiros, por meio eletrônico, com débito das parcelas em conta corrente da autora. Negativação indevida da requerente. Responsabilidade objetiva do banco requerido pelos serviços prestados. Verba indenizatória devida. *Quantum* indenizatório bem mensurado. Recursos desprovidos. Sentença mantida” (TJSP, Apelação 0000676-15.2010.8.26.0125, rel. Des. Ademir Benedito, j. 26-10-2011).

“Administradora de cartão e sistemas de pagamento. Fraude. Recurso. Apelação. Alegação de que a ré tinha o ônus da prova da recusa de pagamento dos titulares de cartão de crédito pelo não reconhecimento da validade das compras devidamente autorizadas por ela não conhecida. Julgamento de recurso com alteração de pedido ou a causa de pedir deduzido na inicial afronta ao princípio do duplo grau de jurisdição e caracteriza julgamento *extra petita*, com violação do disposto nos arts. 128, 264, 460, 514, II, e 515, § 1º, do CPC. Cartão de crédito. Contrato de afiliação. Administradora do Sistema Visanet deve arcar com os valores relativos aos negócios jurídicos por ela autorizados, mesmo que não reconhecidos pelos titulares de cartão, na hipótese de cartões clonados, quando não demonstrado descumprimento pelo empresário vendedor de obrigações contratuais, visto que a responsabilidade pela segurança do sistema Visanet é da administradora que presta esse serviço, com incumbência de prover meios que impeçam a concessão de autorização para vendas realizadas com cartões de crédito clonados. Ausente prova do descumprimento pela autora fornecedora de obrigações contratuais relativamente às vendas devidamente autorizadas pela ré administradora, com base em cartões de crédito colados. Reforma para julgar procedente a ação. Recurso provido” (TJSP, Apelação 0154088-12.2008.8.26.0100, rel. Des. Rebello Pinho, j. 15-8-2011).

DOCUMENTOS E CONTRATOS ELETRÔNICOS. VALIDADE.

Comentários:

O documento eletrônico nada mais é do que suporte digital da comprovação de um fato, que em regra se traduz em uma manifestação de vontade que produzirá seus efeitos jurídicos no mundo real. Para o direito, tem valor de documento todo escrito capaz de gerar compreensão humana. Independe de suporte (pode ser a pedra, o pano, o papel, o HD).

Assim sendo, nada mais natural do que a aceitação gradual e contínua de nossos Tribunais, assim como da sociedade civil, de documentos eletrônicos como prova e instrumento de materialização dos negócios e atos que se procura formalizar.

Ocorre que o contrato eletrônico deve ter os mesmos requisitos de validade do contrato em papel, como o agente capaz. É essencial adequar o modelo de autenticação para gerar prova de autoria e também garantir a integridade do conteúdo do contrato após assinado eletronicamente — que pode ir de um “click-ok” em um termo de uso *online* até o uso de certificado digital e biometria.

“Agravado de instrumento. Execução de título extrajudicial. Contrato de empréstimo bancário. Reprodução digital do contrato original. Exigência de apresentação do original. Desnecessidade validade da certificação digital. 1. Cuida a hipótese de Agravo de Instrumento interposto contra a decisão do juízo a quo, em ação de execução de título extrajudicial, que determinou que o exequente apresentasse o contrato original. 2. Exequente sustenta que o contrato que baseia a execução está de acordo com a certificação digital, denotando a mesma veracidade do documento original, sendo ainda desnecessária a sua juntada, vez que se trata de documento particular. 3. Validade de utilização de documentos eletrônicos devidamente certificados — Lei n. 11.419/2006. Aplicação do art. 365, VI, do Código de Processo Civil. 4. Precedentes deste Tribunal. Dou provimento ao recurso com fundamento no § 1º-A do art. 557 do Código de Processo Civil” (TJRJ, Agravo de Instrumento 0040203-53.2010.8.19.0000, rel. Marcelo Lima Buhatem, j. 24-8-2010).

“Agravado de instrumento. Ação de execução de título extrajudicial. Instrução da inicial com cópia de contrato de empréstimo registrado eletronicamente. Decisão que determinou a vinda aos autos do contrato original ou cópia autenticada. Exigência desnecessária porquanto devidamente registrado no cartório de títulos e docu-

mentos o documento eletrônico. Art. 388, I, do CPC. Jurisprudência deste eg. Tribunal de justiça e do STJ. Recurso a que se dá provimento, de plano” (TJRJ, Agravo de Instrumento 0037938-78.2010.8.19.0000, rel. Luisa Bottrel Souza, j. 18-8-2010).

“Agravado de instrumento tirado contra decisão proferida em execução extrajudicial que determinou a juntada do original do contrato exequendo sob pena de extinção da ação. Inconformismo do banco credor sustentando que a instrução da ação com a cópia do Contrato de Financiamento certificado digitalmente em cartório extrajudicial não obsta o seu direito. Acolhimento. Exibição de cópia do contrato registrada eletronicamente com certificação digital de autenticidade perante cartório extrajudicial. Presunção de autenticidade que emerge da certificação digital, dispensando a juntada do original ou de cópia autenticada. Interpretação do art. 385 do CPC, que deve ser feita em consonância com os avanços da era digital. Inteligência do art. 365, VI, do CPC, c.c. art. 11, § 1º, da Lei n. 11.419/2006 (Informatização do Processo Judicial). Recurso provido” (TJSP, Agravo de Instrumento 990.10.334055-8, rel. Moura Ribeiro, j. 12-8-2010).

“Processual civil. Ação indenizatória cumulada com pedido de tutela antecipada. Danos morais. Renegociação de dívida. Meio eletrônico. Ônus do banco quanto à prova de efetivação do pacto. Valor indenizatório que se reduz. Recurso ao qual se dá provimento com base no art. 557, § 1º-A, do Código de Processo Civil, de forma parcial. I — Incumbe ao banco demonstrar, por meios idôneos, a inexistência ou impossibilidade de fraude, tendo em vista a notoriedade do reconhecimento da possibilidade de violação do sistema eletrônico de saque por meio de cartão bancário e/ou senha. Precedentes do colendo Superior Tribunal de Justiça; II — Ausente a prova do contrato de renegociação firmado entre as partes, e que se sustenta firmado pela via eletrônica, resta indevida a inscrição em órgão de restrição de crédito; III — Quantum indenizatório que se reduz para adequá-lo aos parâmetros da Câmara; IV — Recurso ao qual se dá provimento com amparo no art. 557, § 1º-A, do Código de Processo Civil, de forma parcial” (TJRJ, Apelação 0409927-39.2008.8.19.0001, rel. Admir Pimentel, j. 24-6-2010).

“Agravado de instrumento. Execução de título extrajudicial. Contrato de empréstimo bancário. Reprodução digital do contrato original. Exigência de apresentação do original. Desnecessidade da validade da certificação digital. Cuida a hipótese de Agravo de Instrumento interposto contra a decisão do juízo a quo, em ação de execução de título extrajudicial, determinou que o exequente apresentasse o contrato original. Exequente sustenta que o contrato que baseia a execução está de acordo com a certificação digital, denotando a mesma veracidade do documento original, sendo ainda desnecessária a sua juntada, vez que se trata de documento particular. Vali-

dade de utilização de documentos eletrônicos devidamente certificados. Lei n. 11.419/2006. Aplicação do art. 365, VI, do Código de Processo Civil. Precedentes deste Tribunal. Aplicação do § 1º-A do art. 557 do Código de Processo Civil. Recurso que se dá provimento” (TJRJ, Agravo de Instrumento 0024514-66.2010.8.19.0000, rel. Caetano Fonseca Costa, j. 31-5-2010).

“*Agravo de instrumento. Cumprimento de sentença. Sucessão empresarial. Mesmo ramo de atividade. Mesmos sócios. Sucessão divulgada em sítio eletrônico da sucessora. Indícios suficientes. Decisão reformada.* A sucessão empresarial é fato que deve ser devidamente comprovado, não podendo ser presumido por simples indícios. Presentes fortes indícios de sucessão empresarial entre as pessoas jurídicas demandadas, ou, ainda, confusão patrimonial, impõe-se o deferimento do pedido de inclusão da suposta empresa sucessora no polo passivo da lide” (TJMG, Recurso Cível 0256599-38.2001.8.13.0313, rel. Irmair Ferreira Campos, j. 11-3-2009).

“*Ação monitória. Cópia digital documento. Autenticidade. Medida Provisória n. 2.200/2001. Documentos forma eletrônica. Possibilidade.* A Medida Provisória n. 2.200, de 28-6-2001, se propõe a ‘garantir autenticidade, integridade e validade jurídica de documentos em forma eletrônica, mediante a criação de uma Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)’. Esta MP garante ao documento eletrônico a força de presunção verdadeira quanto aos seus signatários” (TJMG, Recurso Cível 5415691-77.2009.8.13.0024, rel. José Affonso da Costa Côrtes, j. 11-2-2009).

“*Agravo de instrumento. Processo civil. Competência territorial. Internet. Contrato eletrônico. Serviço de atribuição de ISBN. Obrigação de fazer e indenização.* É competente o foro do lugar em que expedida a proposta contratual (CPC art. 100, V, a, c/c CC art. 435). Proposta que se considera expedida na sede da pessoa jurídica proponente (LICC [hoje, LINDB] art. 9º, § 2º). Decisão mantida por outro fundamento legal. Recurso improvido” (TJSP, Agravo de Instrumento 677.025-4/1-00, rel. Egidio Giacoia, j. 1-12-2009).

“*Agravo de instrumento. Ausência de peças obrigatórias. Certidão de intimação. Juntada de informativo eletrônico. Ausência de fé pública.* Conforme disposto no art. 525 do Código de Processo Civil, a petição de agravo será obrigatoriamente instruída com cópia da certidão da respectiva intimação da decisão agravada. A cópia do Diário Eletrônico não tem o condão de substituir a cópia da certidão de publicação, por ausência de fé pública. Recurso não provido” (TJMG, Recurso Cível 1142637-54.2009.8.13.0114, rel. Cabral da Silva, j. 11-3-2010).

“*Ação de cobrança. Contrato de prestação de serviços educacionais aderido via Internet. Validade. Litigância de má-fé. Inocorrência.* Como se sabe, grande parte das universidades utiliza o sistema via Internet para, visando a facilitação dos serviços e a maior comodidade dos próprios alunos, contratar matrículas nos cursos por elas oferecidos. Tal sistema não apresenta qualquer ilegalidade ou abusividade. Isso porque, para aderir ao contrato, deve o aluno clicar em *links* e confirmar senha para efetivar a matrícula, demonstrando, de forma inequívoca, a vontade de contratar. Ausente a prática de qualquer conduta que caracterize litigância de má-fé, não há que se falar em sanção a esse título” (TJMG, Apelação Cível 1.0024.06.236128-2/001, rel. Des. Elpídio Donizetti, DJ 9-2-2009).

“*Processual civil. Agravo regimental em agravo regimental em agravo de instrumento. Agravo regimental intempestivo. Transmissão por meio eletrônico. Documento inacessível. Responsabilidade do remetente. Agravo improvido.* I — A responsabilidade pela integridade dos arquivos remetidos eletronicamente é do remetente. II — Agravo regimental improvido” (STF, AgR-AgR AI 589982, rel. Min. Ricardo Lewandowski, j. 13-5-2008).

“*Agravo de instrumento. Tempestividade. Comprovante de prorrogação do prazo sem assinatura.* 1. Intempestivo o agravo de instrumento interposto após o decurso do prazo legal. 2. Documento destituído de assinatura hológrafa ou eletrônica não serve como meio de prova da suspensão do prazo recursal. Inobservância do contido na Súmula 385 desta Corte superior. Agravo de instrumento não conhecido” (TST, AIRR 1390/2005-009-13-41.1, rel. Min. Lelio Bentes Corrêa, publ. 6-2-2009).

“*Assinatura eletrônica. Validade.* O Provimento GP/CR 14/2006 (o qual revogou a Portaria GP/CR 24/05), regulamentado pelo Provimento GP/CR 05/08 (art. 345 e parágrafo), instituiu, no âmbito da Justiça do Trabalho da 2ª Região, o Sistema Integrado de Protocolização de Documentos Físicos e Eletrônicos (Sis-Doc), possibilitando a utilização da Internet para a prática de atos processuais sob a forma de petição escrita, dependendo apenas da identidade digital do usuário, sem a necessidade de ratificação posterior (art. 3º, §§ 1º e 5º). *In casu*, a peça recursal coligida às fls. 111/117 demonstra a existência da propalada assinatura via SisDoc, evidenciando sua validade jurídica” (TRT2, RO 0793200605802007, rel. Paulo Augusto Camara, j. 29-7-2008).

“*Agravo de Instrumento. Ação de Retificação de Assento e Nascimento.* Apresentação de Certidão da Justiça Federal extraída do sítio eletrônico oficial da Justiça Federal de São Paulo. Inteligência do art. 365, VI, do CPC. Observância à

Ordem de Serviço n. 03/2007. Decisão reformada. Recurso Provido” (TJSP, Agravo de Instrumento 994071160774, rel. Des. Octavio Helene, j. 4-11-2008).

“Indenização. Existência de fundamentação. Livre apreciação da prova. Valoração. Convencimento do juiz. Contrato eletrônico. Inexistência de forma prescrita em lei. Validade. O recurso deve ser conhecido quando suas razões encerram fundamentos de fato e de direito. A livre apreciação da prova, considerada a lei e os elementos constantes dos autos, é um dos cânones do processo, cabendo ao Julgador atribuir-lhe o valor de acordo com o seu convencimento. A contratação de empréstimo bancário pela via eletrônica com manifestação de vontade através de confirmação de mensagens e utilização de cartão magnético e senha é válida, por inexistir forma prescrita em lei” (TJMG, Apelação Cível 1.0024.06.153382-4/001, rel. José Amâncio, j. 5-3-2008).

“Ação de cobrança. Mensalidade escolar. Contrato de prestação de serviços. Documento eletrônico. Possibilidade. Encargos. Legalidade. A despeito de o contrato de prestação de serviços não conter a assinatura da requerida, tal fato não é apto a invalidar o referido ajuste, tendo em vista que o contrato de prestação de serviços educacionais é informal e não exige forma prescrita em lei, podendo até ser firmado verbalmente. O contrato de prestação de serviços, juntado aos autos, ainda que desprovido de assinatura da ré, é suficiente para provar a realização do ajuste, visto que os documentos eletrônicos gozam de valor probante e o doc. de f. 06-09 demonstra que a requerida efetivamente aderiu ao aludido contrato, via Internet. Não há ilegalidade ou abusividade da cláusula que prevê, para o caso de inadimplemento, a incidência de multa de 2%, juros de mora de 1%, atualização monetária pelo IGP-M” (TJMG, Ap. 2.0000.00.450396-4/000, rel. Pedro Bernardes, j. 19-10-2004).

9 — NEGÓCIOS VIRTUAIS E QUESTÕES TRIBUTÁRIAS

SITES DE LEILÃO NA INTERNET

Comentários:

Os sites de leilão na Internet são uma das modalidades de negócio que mais crescem atualmente. A dificuldade de assemelhar essa modalidade de negócio ao leilão tradicional é que implica a grande maioria dos litígios.

Importante dizer que o leilão tradicional implica a responsabilidade do leiloeiro com relação ao produto que está sendo vendido, avalizando a mercadoria. Todavia, assim não ocorre com o leilão virtual, que se apresenta como um mero espaço/ponto de encontro de terceiros interessados em vender ou trocar suas mercadorias.

Como é sabido, há nítido caráter de leilão, com comissão e várias outras características próprias do negócio leiloeiro, o que não tem afastado as tentativas de total exclusão da responsabilidade pelos espaços que conhecemos como leilões virtuais.

Há agora os sites de compra coletiva, que também estão sujeitos às regras do Código de Defesa do Consumidor.

“Reparação de danos materiais. Comércio eletrônico. Internet. Site de anúncios. Que barato — Grupo Busca Pé. Produto pago e não enviado. Fraude ao oferecer o produto, apto a iludir o comprador. Responsabilidade da empresa intermediadora. Dever de indenizar. Sentença mantida. Recurso improvido” (TJRS, Recurso Cível 71002372514, 2ª Turma Recursal Cível, rel. Vivian Cristina Angonese Spengler, j. 14-7-2010).

“Preliminar. A empresa apelante é fornecedora de serviço, enquadrando-se na forma especificada no art. 3º, caput, do CDC e, assim sendo, participando, efetivamente, da ‘cadeia de consumo’ tem ela efetiva responsabilidade pelos serviços disponibilizados aos seus consumidores. Princípio da solidariedade da responsabilidade dos fornecedores pela ocorrência de dano na relação de consumo. Arts. 7º, parágrafo único, e 25, parágrafo único, ambos do CDC. Preliminar rejeitada. (...) por danos morais. Recurso do autor apelante não provido para esse fim. *Indenização. Danos materiais existência e comprovação. Serviços de internet prestados de forma inadequada. Art. 14 do CDC. Efetiva existência de relação de consumo.* A empresa que disponibiliza site de intermediação para compra e venda de produtos tem o dever de fiscalizar a idoneidade das empresas que oferecem seus produtos em tal site. Se a empresa que disponibiliza tais serviços em seu site é negligente na fiscalização da

idoneidade dessas empresas vendedoras responde pelos prejuízos suportados pelos consumidores que utilizam o seu *site*. Danos materiais existentes. Recurso da empresa apelante não provido para esse fim” (TJSP, Apelação 7390505-0, rel. Des. Roberto Mac Craken, j. 22-10-2009).

“Comércio eletrônico. Ação de indenização por danos materiais proposta por consumidor, vítima de fraude praticada por terceiro, em face de empresa de intermediação de negócios via Internet denominada ‘Mercado Livre’. Aplicação do CDC por se tratar de prestação de serviços. Excludente de responsabilidade decorrente de culpa exclusiva do consumidor, que não observou os procedimentos de segurança antes de liberar a mercadoria. *E-mail* fraudulento enviado pelo suposto comprador, sem a participação da empresa intermediadora, noticiando a efetivação do pagamento e solicitando liberação da mercadoria. Informações claras e precisas constantes do *site* da recorrente alertando para a necessidade de verificação do pagamento na própria página do ‘Mercado Livre’ antes da liberação da mercadoria e da autenticidade do endereço da página recebida por *e-mail* para que o usuário não corra o risco de ser vítima de *e-mail* falso em nome do *site*. Inexigibilidade, porém, da comissão de intermediação. Sentença parcialmente reformada. Recurso provido em parte” (TJSP, Colégio Recursal, RI 030635, rel. Juiz Jorge Tosta, DOJ 5-5-2008).

“Apelação cível. Indenizatória por danos materiais e morais. Relação de consumo. Responsabilidade do fornecedor de serviço exposição de produto via Internet. Sistema que permitiu o envio de *e-mail* falso, induzindo o consumidor a erro. Responsabilidade objetiva. Art. 14 da Lei n. 8.078/90. *Quantum* indenizatório que se coaduna ao patamar sedimentado neste Tribunal de Justiça, atendendo a indenização por danos morais às suas funções educativa e compensatória chancela do princípio da proporcionalidade e razoabilidade. Pretensão recursal manifestamente improcedente. Negativa de seguimento. Art. 557, *caput*, do CPC” (TJRJ, Acórdão de Apelação 2008.001.52269, rel. Des. Mario Guimarães Neto, j. 22-1-2009).

“*Medida cautelar*. Abstenção de veiculação de anúncio de venda de produtos da marca ‘Diesel’ pela Internet, sob pena de multa diária. Liminar concedida. Ordem mantida. Pleito que encontra lastro em contrato de distribuição exclusiva de produtos importados. Oferta em *site* de comércio eletrônico de mercadorias contrafeitas com essa marca, ou originais ilegalmente adentrados no país. Atividade deste, que embora lícita, contribui para a prática desses ilícitos, com os quais auferir vantagem econômica. Requerida que admite a impossibilidade técnica de excluir as ofertas de produtos ilegais. *Fumus boni juris* e *periculum in mora* bem demonstrados. Recurso desprovido” (TJSP, Cautelar 448.555-4/4, rel. Des. Galdino Toledo Junior, j. 22-5-2007).

O CONSUMIDOR NA INTERNET

Comentários:

O consumidor na Internet tem os mesmos direitos que o consumidor que se dirige a uma loja física. Assim, independentemente do local em que se consuma qualquer negócio jurídico entre consumidor e empresa, ter-se-á a aplicação do Código de Defesa do Consumidor. Mas cabe a ele se informar antes de comprar, ler as políticas do *site* antes de confirmar a compra, principalmente no que diz respeito à troca ou à devolução.

“Reparação de danos. Compra pela Internet. Atraso na entrega. Promessa de entrega de geladeira antes do final do ano. Descumprimento do acordado. Transfornos decorrentes da falta do bem durante os festejos de fim de ano, em que o autor tinha visitas em casa. Peculiaridades do caso concreto. Lesão de ordem extrapatrimonial configurada. Recurso improvido” (TJRS, Recurso Cível 71002522092, rel. Fernanda Carravetta Vilande, j. 23-6-2010).

“*Responsabilidade civil. Ação de indenização por danos morais. Envio de mensagem através de página de relacionamento na Internet (Orkut). Dano moral configurado. Indenização por danos morais concedida no valor de R\$ 2.000,00, que se adequa ao parâmetro utilizado pela turma nas indenizações concedidas em casos semelhantes. Dano moral restou configurado, visto que comprovada a mensagem enviada (fls. 12 e 13) pela ré através da página de relacionamento na Internet ‘Orkut’ efetuando uma cobrança. Ademais, a parte ré não comprovou suas alegações de que a parte autora teria forjado tal situação. Não há como negar que tal atitude mostrou-se abusiva, uma vez que há outros meios de realizar-se uma cobrança, sem que se exponha a imagem de outrem. No caso concreto restou evidenciado o abalo à personalidade da requerente, eis que a página de relacionamento na Internet é pública e os dados ficam acessíveis a qualquer pessoa. A indenização por dano moral possui função satisfatória, procurando, muito mais, a recompensa pela dor e sofrimento causados do que a restituição integral à ofensa causada. Justamente por isso, tem-se que o valor indenizatório não deve ser uma fonte de enriquecimento para a indenizada. A requerida, na condição de responsável pela exibição da imagem da demandante, é responsável pelos danos advindos de tal situação. Nesta esteira, o valor de R\$ 2.000,00, arbitrado em primeira instância, mostra-se justo e eficiente para preencher os objetivos das indenizações por dano moral, estando de acordo com os princípios da proporcionalidade e razoabilidade, bem como os parâmetros utilizados pelas Turmas Recursais, em casos análogos. Sentença mantida por seus próprios fundamentos. Recurso improvido” (TJRS, Recurso Cível 71002407856, rel. Luís Francisco Franco, j. 23-2-2010).*

“Civil. (...) Compra e venda. Falha na entrega do produto. Cancelamento da avença. Composição das partes quanto danos materiais. Indenização pecuniária por violação da honra do consumidor. (...) 3. (...) No caso em tela, o serviço deficiente da ré ficou no plano patrimonial, não ensejando dano extrapatrimonial. Embora tenha o demandante experimentado desassossego decorrente da realização de serviço de má qualidade, entende-se que os indivíduos devem suportar não apenas a comodidade da vida em sociedade, como também os aborrecimentos dela provenientes (...)” (TJDF, Recurso Inominado 2007091012852, rel. Donizeti Aparecido, j. 29-4-2008).

“Anúncio pela Internet. (...) Apelante que ao se dirigir ao estabelecimento comercial descobre que não existia tal promoção. Apelada que demonstra a ocorrência de um equívoco, poucas horas após desfeito com a divulgação de errata pelo mesmo veículo. Concomitante comunicação ao PROCON acerca do ocorrido. Ausência de dolo de enganar o consumidor (...)” (TJRJ, Apelação 2008.001.20273, rel. Helda Lima Meireles, j. 13-5-2008).

“Direito civil e do consumidor. Internet. Relação de consumo. Incidência do CDC. Gratuidade do serviço. Indiferença. Provedor de conteúdo. Fiscalização prévia do teor das informações postadas no site pelos usuários. Desnecessidade. Mensagem de conteúdo ofensivo. Dano moral. Risco inerente ao negócio. Inexistência. Ciência da existência de conteúdo ilícito. Retirada imediata do ar. Dever. Disponibilização de meios para identificação de cada usuário. Dever. Registro do número de IP. Suficiência. 1. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei n. 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo ‘mediante remuneração’ contido no art. 3º, § 2º, do CDC deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. 3. A fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na web por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra os dados e imagens nele inseridos. 4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/2002. 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de

conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por culpa in omittendo. 7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo, que registra o número de protocolo na Internet (IP) dos computadores utilizados para o cadastramento de cada conta, mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de Internet. 8. Recurso especial a que se nega provimento” (REsp 1.193.764/SP, rel. Nancy Andrighi, j. 14-12-2010, DJe 8-8-2011).

“Civil e consumidor. Internet. Relação de consumo. Incidência do CDC. Gratuidade do serviço. Indiferença. Provedor de conteúdo. Fiscalização prévia do teor das informações postadas no site pelos usuários. Desnecessidade. Mensagem de conteúdo ofensivo. Dano moral. Risco inerente ao negócio. Inexistência. Ciência da existência de conteúdo ilícito. Retirada imediata do ar. Dever. Disponibilização de meios para identificação de cada usuário. Dever. Registro do número de IP. Suficiência. 1. A exploração comercial da Internet sujeita as relações de consumo daí advindas à Lei n. 8.078/90. 2. O fato de o serviço prestado pelo provedor de serviço de Internet ser gratuito não desvirtua a relação de consumo, pois o termo ‘mediante remuneração’, contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, de modo a incluir o ganho indireto do fornecedor. 3. A fiscalização prévia, pelo provedor de conteúdo, do teor das informações postadas na web por cada usuário não é atividade intrínseca ao serviço prestado, de modo que não se pode reputar defeituoso, nos termos do art. 14 do CDC, o site que não examina e filtra os dados e imagens nele inseridos. 4. O dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/2002. 5. Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve o provedor agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada. 6. Ao oferecer um serviço por meio do qual se possibilita que os usuários externem livremente sua opinião, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada manifestação uma autoria certa e determinada. À ótica da diligência média que se espera do pro-

vedor, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do *site*, sob pena de responsabilização subjetiva por culpa *in omittendo*. 7. Ainda que não exija os dados pessoais dos seus usuários, o provedor de conteúdo que registra o número de protocolo (IP) na Internet dos computadores utilizados para o cadastramento de cada conta mantém um meio razoavelmente eficiente de rastreamento dos seus usuários, medida de segurança que corresponde à diligência média esperada dessa modalidade de provedor de serviço de Internet. 8. Recurso especial provido” (REsp 1.186.616/MG, rel. Nancy Andrighi, j. 23-8-2011, DJe 31-8-2011).

“*Ação de reparação de danos*. Compra e venda de bem móvel por meio da Internet. Sentença devidamente fundamentada, com clara exposição das razões de decidir. Inexistência de afronta ao mandamento contido no art. 93, IX, da Constituição Federal. Elementos de prova suficientes para a formação da convicção. Julgamento antecipado que não configura cerceamento de defesa e, ao revés, consagra o princípio da razoável duração do processo. Compreensão do art. 330, I, do CPC. Empresa que se insere no mercado de prestação de serviço, disponibilizando *site* na Internet para, mediante remuneração, facilitar negócios, não está imune às intercorrências advindas. Formação da obrigação de suportar, solidariamente com aquele que violou direito, o prejuízo causado ao consumidor. Ausência de cautela básica, que de todo se exige, que estabelece a culpa concorrente do consumidor. Dano moral somente se forma quando há violação ao direito de outrem, sem que para tanto este concorra para o resultado. Desídia consistente que veda a imposição de indenização por danos morais. Recurso do corréu desprovido. Recurso do autor parcialmente provido” (TJSP, Apelação 9209343-73.2006.8.26.0000, rel. Des. Dimas Rubens Fonseca, j. 11-10-2011).

“*Apelação cível. Responsabilidade civil. Provedor de Internet. Mercado livre. Opção pela modalidade ‘mercado pago’*. Mensagem eletrônica (e-mail) enviado por terceiro fraudador como se fosse o provedor prestador do serviço. Risco intrínseco à atividade que configura fortuito interno, ensejando a responsabilidade do fornecedor de serviços. Dever de informar o risco não satisfatoriamente cumprido. Ausência de dano moral. O risco de um terceiro obter as informações e enviar mensagem eletrônica como se fosse o provedor deveria ser claramente advertido, assim como a imposição de que o consumidor-vendedor verifique no *site* sua conta antes de remeter o produto. Não pode o fornecedor de serviços se utilizar de fontes grandes e claras em cores chamativas no seu *site* para alardear as qualidades de seu produto e deixar as informações sobre os riscos e medidas de segurança para serem explicitadas apenas no contrato de adesão. Se a informação não foi comprovadamente forne-

cida de maneira adequada ao consumidor — ônus que incumbe ao fornecedor —, o risco da atuação fraudulenta de terceiro deve recair sobre o fornecedor, o qual deve responder perante o consumidor e buscar o terceiro em ação regressiva. Fato ensejador de dano patrimonial, pelo envio da mercadoria sem recebimento do preço prometido, mas não de dano moral. Recurso a que se dá parcial provimento” (TJRJ, Apelação Cível 0200216-28.2007.8.19.0001, rel. Des. Marcia Ferreira Alvarenga, j. 13-4-2011).

“*Apelação. Ônus da prova. Contrato de prestação de serviços. Venda de produtos pelo site. Ausência de prova da contratação. Teoria do risco proveito. Dano moral. Configurado. Quantum. Proporcionalidade*. O ônus de provar a celebração do negócio jurídico é do réu, já que é impossível ao requerente provar que não efetuou o anúncio no *site* réu. A referida prova é tida pela doutrina como prova diabólica, já que trata de uma prova negativa no qual é impossível a sua produção. O sistema de contratação dos anúncios via Internet é frágil, já que possibilita a fraude de terceiros. A culpa da empresa ré está configurada pelo fato de disponibilizar um sistema frágil de contratação que coloca em risco o direito de outrem. Trata-se da teoria do risco proveito prevista no art. 927, parágrafo único, do Código Civil. Se o sistema disponibilizado falhou, a empresa da ré deve arcar com os prejuízos causados a parte, principalmente considerando que a mesma lucra pela venda realizada. Os danos morais estão configurados, já que o autor foi acusado de vender um aparelho celular e não entregá-lo, fato este que denegriu a honra do requerente. O valor da reparação por danos morais visa recompor o abalo sofrido. Deve ser arbitrado com proporcionalidade, tendo em vista a extensão do dano e as condições econômicas do violador do dever de cuidado” (TJMG, Apelação Cível 1.0625.10.000297-5/001, rel. Des. Tibúrcio Marques, j. 17-2-2011).

“Consumidor e processual civil. Ação indenizatória. Fraude em compra e venda realizada pela Internet. ‘Mercado Livre’. Sentença de improcedência. Apelo da autora. Utilização dos serviços oferecidos pelo réu para anunciar valiosa joia familiar. Autora que afirmou ter utilizado o serviço denominado “mercado pago”, recebendo um *e-mail* do réu confirmando o pagamento pelo terceiro adquirente do produto. Prova pericial em sentido diametralmente inverso. Autora que recebeu um *e-mail* fraudado pelo terceiro, que simulou ter realizado o pagamento. Aspecto gráfico que indica a origem fraudulenta do *e-mail*. Autora que não comprovou a conduta ilícita do réu, sendo este um ônus seu (art. 333, I, CPC), ainda que diante de relação consumerista. Precedentes deste tribunal. Sentença que se mantém. Desprovimento do apelo” (TJRJ, Apelação 0014393-28.2005.8.19.0202, rel. Des. Luiz Fernando de Carvalho, j. 23-3-2011).

COMPRAS COLETIVAS

“Consumidor. Responsabilidade civil objetiva. *Site* de compra coletiva. Oferta de aparelho celular vinculado a plano de utilização da linha telefônica. Aquisição de cupom sem a respectiva entrega do produto. Falha na prestação do serviço. Dano moral configurado. Precedentes deste TJERJ. Responsabilidade solidária dos integrantes da cadeia de consumo. Verba reparatória fixada em conformidade com os princípios da proporcionalidade e da razoabilidade. Recursos a que se nega seguimento” (TJRJ, Apelação Cível 0001387-41.2011.8.19.0202, rel. Des. Marco Antonio Ibrahim, j. 12-9-2011).

“Apelação cível. Direito do consumidor. Compra de aparelho celular realizada pela Internet. Solidariedade entre o *site* de compra *online* e a empresa prestadora de serviço de intermediação comercial por meio eletrônico quanto à finalização da transação. Não entrega do produto. Responsabilidade solidária de todos que integram a ‘cadeia de fornecimento’. Risco do empreendimento. Circunstância em que o autor, até a presente data, não recebeu a restituição. Situação que desborda do mero descumprimento contratual, tornando inaplicável a Súmula 75 do TJRJ. Frustração da legítima expectativa do consumidor reforma parcial da sentença. (...)” (TJRJ, 4ª Câmara Cível, Apelação Cível 2193188-70.2011.8.19.0021, rel. Des. Marcelo Lima Buhatem, j. 26-8-2011).

“Ação indenizatória. Compra realizada através de site na Internet. Cancelamento unilateral. Produto divulgado. Caráter vinculativo. Princípio da confiança. Dano moral configurado. Quantum fixado em observância aos princípios da razoabilidade e proporcionalidade. Decisão monocrática com fulcro no art. 557, caput, do CPC, que nega seguimento aos recursos. A legislação consumerista vinculou o fornecedor àquilo que por ele é ofertado, protegendo, dessa forma, o consumidor. A ré deveria ter verificado o estoque ou a possibilidade de reposição do produto antes de oferecê-lo ao consumidor, o que não ocorreu na hipótese” (TJRJ, Apelação Cível 0151516—84.2008.8.19.0001, rel. Des. Vera Maria Soares Van Hombeeck, j. 6-4-2011).

CONTRAFAÇÃO — VENDA DE CDS “PIRATAS” NA INTERNET

“A prova colhida é, pois, claríssima no tocante à violação de direito autoral. O réu copiava sem autorização e disseminava ao público fonogramas da banda musical em tela. Resta evidente, também, e isso anota a prova pericial, assim como a fartíssima prova documental, que o acusado tinha o intuito de lucro e efetiva-

mente lucrou com as verdadeiras transações comerciais havidas. De se notar que no *site* em que propagandeava a venda (e não a mera remessa por espírito de aficionado) dos fonogramas, em momento algum havia anotação de que se tratava de fã-clube ou de que as transações seriam efetivadas apenas com amigos ou outros aficionados pelo citado grupo. Ademais, indica-se que o valor fixado para o negócio referia-se à própria venda do disco compacto, e não apenas às despesas postais, tanto assim que há mensagens envidadas pelo acusado, como ocorre a fls. 22/23, em que, após indicar o valor da transação comercial, anotava-se que a tarifa de correio já estava incluída no preço, além de haver pura propaganda do negócio, ao público em geral, lembrando que a oportunidade de compra era única, eis que se poderia adquirir a baixo custo a coleção integral, ao passo que um disco simples (original, é evidente) teria custo bem maior. O laudo pericial nos dados eletrônicos relativos ao réu e os inúmeros depósitos em sua conta corrente reforçam a certeza de violação de direito autoral com intuito de lucro. Inviável a desclassificação para a forma simples do delito, portanto. Não há, ademais, prescrição a ser declarada. Consta que o réu obteve cópias de todas as músicas comercializadas pelo antigo grupo musical *The Beatles* e, como possuía acesso cadastrado a Internet, elaborou página virtual em que passou a oferecer, para aquisição, a Coleção Completa dos Beatles em MP3, primeiro por dez reais e após por vinte reais, mediante depósito no Banco Itaú, em conta de sua titularidade” (TJSP, Juízo da 18ª Vara Criminal, Proc. 583.50.2003.065972-5, MM. Juiz Marcello O. L. Guimarães, j. 13-8-2008).

ICMS E SOFTWARE

Comentários:

O Imposto de Circulação de Mercadorias e Serviços (ICMS) não incide nos serviços de comercialização de *software*, a não ser que estes sejam vendidos por prateleira, ou seja, disponibilizados em meio físico. Diferente seria, e o é, quando o programa é repassado apenas pela licença de sua utilização, vez que não se pode esquecer que se trata de uma criação intelectual. Tem crescido a discussão sobre o ICMS na venda pela Internet, bem como sobre a incapacidade de se tributar um bem que não circule fisicamente (ex.: *download*).

“Processual civil. Recursos. Agravo em julgamento monocrático. 1. Não cabe modificar a decisão em agravo, salvo quando comprovada a sua incorreção no plano material, o que não se coaduna com a jurisprudência pacífica da Corte Superior sobre os pontos abordados de acordo com a seguinte ementa originária: Direito tributário. ISS. Cessão de uso de software. Mandado de segurança. Pedido de liminar de suspensão da exigibilidade do crédito tributário. Segundo a jurisprudência das Cortes

Superiores, incide o ISS sobre as operações com programas de computador desenvolvidos por encomenda, para determinado cliente, de forma personalizada. Quando o programa é criado e vendido de forma impessoal, adquirido pelos clientes como uma mercadoria qualquer, há uma venda, gravada com o ICMS. Situação em que não foram trazidos elementos documentais suficientes, que permitissem definir a natureza da cessão realizada pela empresa impetrante, traduzida nas cópias das notas fiscais acostadas, se customizada ou generalizada. Hipótese de negativa de seguimento. 2. Agravo desprovido” (TJRS, Agravo 70032826513, rel. Rejane Maria Dias de Castro Bins, j. 19-11-2009).

“*Tributário. Estado de São Paulo. ICMS. Programas de computador (software). Comercialização.* No julgamento do RE 176.626, Min. Sepúlveda Pertence, assentou a Primeira Turma do STF a distinção, para efeitos tributários, entre um exemplar *standard* de programa de computador, também chamado ‘de prateleira’, e o licenciamento ou cessão do direito de uso de *software*. A produção em massa para comercialização e a revenda de exemplares do *corpus mechanicum* da obra intelectual que nele se materializa não caracterizam licenciamento ou cessão de direitos de uso da obra, mas genuínas operações de circulação de mercadorias, sujeitas ao ICMS. Recurso conhecido e provido” (STF, RE 199.464, rel. Ilmar Galvão, j. 2-3-1999).

“I — Recurso extraordinário: prequestionamento mediante embargos de declaração (Súm. 356). A teor da Súmula 356, o que se reputa não prequestionado é o ponto indevidamente omitido pelo acórdão primitivo sobre o qual ‘não foram opostos embargos declaratórios’. Mas se, opostos, o Tribunal *a quo* se recuse a suprir a omissão, por entendê-la inexistente, nada mais se pode exigir da parte (RE 210.638, Pertence, DJ 19.6.98). II. RE: questão constitucional: âmbito de incidência possível dos impostos previstos na Constituição: ICMS e mercadoria. Sendo a mercadoria o objeto material da norma de competência dos Estados para tributar-lhe a circulação, a controvérsia sobre se determinado bem constitui mercadoria é questão constitucional em que se pode fundar o recurso extraordinário. III. Programa de computador (*software*): tratamento tributário: distinção necessária. Não tendo por objeto uma mercadoria, mas um bem incorpóreo, sobre as operações de ‘licenciamento ou cessão do direito de uso de programas de computador’ ‘matéria exclusiva da lide’, efetivamente não podem os Estados instituir ICMS: dessa impossibilidade, entretanto, não resulta que, de logo, se esteja também a subtrair do campo constitucional de incidência do ICMS a circulação de cópias ou exemplares dos programas de computador produzidos

em série e comercializados no varejo — como a do chamado ‘*software* de prateleira’ (*off the shelf*) — os quais, materializando o *corpus mechanicum* da criação intelectual do programa, constituem mercadorias postas no comércio” (STF, RE 176.626, rel. Sepúlveda Pertence, DJ 11-12-1998).

PROVEDORES DE ACESSO. NÃO INCIDÊNCIA DE ICMS.

Comentários:

É pacífico nos Tribunais Superiores que o Imposto de Circulação de Mercadorias e Serviços (ICMS) não incide nos serviços dos provedores de acesso à Internet, uma vez que não se trata de serviço de comunicação nem tampouco serviço de valor adicionado, além de faltar previsão e sua incidência à Lei Complementar n. 87, de 13-9-1996.

SÚMULA 334, STJ: O ICMS não incide no serviço dos provedores de acesso à Internet.

“*Tributário. ICMS. Provedor de internet. Não incidência.* 1. O ICMS não incide no serviço dos provedores de acesso à Internet (Súmula 334/STJ). 2. Agravo Regimental não provido” (STJ, 2ª Turma, AgRg no Ag 1.174.206/RJ, rel. Min. Herman Benjamin, j. 1-12-2009, DJe 11-12-2008).

“*Recurso especial. Tributário. ISS. Provedores de acesso à Internet. Não incidência. Recurso desprovido.* 1. A incidência de ISS pressupõe o não cabimento de ICMS, por força de expressa previsão constitucional (art. 156, III). Assim, afastada a incidência de ICMS sobre os serviços prestados pelos provedores de acesso à Internet, cabe analisar se esses se enquadram nos serviços de qualquer natureza, disciplinados no Decreto-Lei n. 406/68, com as alterações introduzidas pela Lei Complementar n. 56/87, para fins de incidência de ISS. 2. O Superior Tribunal de Justiça firmou orientação no sentido de que a lista de serviços anexa ao referido decreto-lei possui um rol taxativo e exaustivo, de modo que é apenas possível uma interpretação extensiva dos itens nela contidos, para o enquadramento de serviços idênticos aos ali expressamente previstos, mas com nomenclatura diversa. 3. Os provedores de acesso à Internet executam serviço de valor adicionado, isto é, atividade de monitoramento do acesso de usuários e de provedores de informações à rede mundial de computadores, colocando à sua disposição os dados

ali existentes. Desse modo, o serviço prestado pelo provedor é apenas o fornecimento da infraestrutura para que o usuário possa acessar a Internet e, por conseguinte, as informações nela contidas. 4. Não há previsão no Decreto-Lei n. 406/68, com suas alterações posteriores, em que se possa incluir os serviços prestados pelos provedores de acesso à Internet entre aqueles sujeitos à incidência de ISS. Isso, porque, conforme anteriormente salientado, esta Corte de Justiça, no julgamento do EREsp 456.650/PR, consignou que a atividade realizada pelo provedor de acesso à Internet é serviço de valor adicionado, constituindo um acréscimo ao serviço de telecomunicações. No entanto, a lista de que trata o decreto-lei supramencionado não incluiu, em seu rol taxativo, os referidos serviços de valor adicionado; além disso, não há nenhuma identidade entre esse serviço e os demais nela expressamente previstos. 5. Não se cogita, conforme pretende o recorrente, sua inclusão nos itens 22 (vetado), 24, 40, 50 e 74 do referido decreto-lei. O item 24 prevê, em síntese, a incidência de ISS sobre os serviços de 'análises, inclusive de sistemas, exames, pesquisas e informações, coleta e processamento de dados de qualquer natureza'; o item 40 dispõe que essa exação relaciona-se aos serviços de 'ensino, instrução, treinamento, avaliação de conhecimentos, de qualquer grau ou natureza'; o item 50 estabelece relação com serviços de 'agenciamento, corretagem ou intermediação de bens móveis e imóveis não abrangidos nos itens 45, 46, 47 e 48'; o item 74 menciona serviços de 'instalação e montagem de aparelhos, máquinas e equipamentos, prestados ao usuário final do serviço, exclusivamente com material por ele fornecido'. 6. Da análise do item 24, constata-se não haver nenhuma identidade entre o serviço prestado pelo provedor (fornecimento de infraestrutura para o acesso à rede Internet) e os serviços de análise de sistemas (estudo de processos para aplicação de tecnologia de informação e de comunicação), de coleta e processamento de dados (organização de dados em computador a fim de obter informação sistematizada) e de informações. Na hipótese, os provedores apenas possibilitam o acesso dos usuários às informações constantes da Internet. Assim, eles apenas as recebem da rede e as retransmitem ao usuário conectado. Por outro lado, o serviço prestado pelo provedor também não se enquadra nas hipóteses previstas nos itens 40, 50 e 74, os quais, mesmo se interpretados extensivamente, estão totalmente dissociados da atividade exercida pelos provedores de acesso à Internet. 7. Recurso especial desprovido. *Petição apresentada por P. Ltda. Julgamento da apelação cível. Incidência de ICMS sobre o serviço prestado pelos provedores de acesso à Internet. Ausência de interposição de recurso especial oportunamente. Preclusão. Vedação de reformatio in pejus. Indeferimento do pedido.* 1. O Tribunal de Justiça estadual, no julgamento da apelação cível, entendeu devida a incidência de ICMS sobre o serviço prestado pelos provedores de aces-

so à Internet, autorizando, por conseguinte, o Estado de Minas Gerais a levantar os depósitos efetuados pela empresa em sede de ação de consignação em pagamento. Em face desse julgado, a empresa ora recorrida — P. Ltda. — não interpôs recurso especial. Todavia, operada a preclusão, veio, por simples petição, nos autos do presente recurso especial, apresentado pelo Município de Belo Horizonte, requerer a exclusão da tributação do ICMS e, conseqüentemente, a extinção de sua obrigação tributária para com o Estado de Minas Gerais e, enfim, o levantamento dos valores por ela depositados em juízo. 2. Configurada a preclusão temporal e consumativa, nos termos dos arts. 183 e 473 do Código de Processo Civil, é incabível o acolhimento das razões da empresa, apresentadas com nítida finalidade recursal. 3. Embora o acórdão proferido pela Corte de origem esteja em desconformidade com a jurisprudência deste Tribunal Superior (Súmula 334/STJ), não pode ser reformado, sob pena de se incorrer em *reformatio in pejus*, vedada pelo ordenamento jurídico pátrio. 4. Petição indeferida. Manutenção das conclusões do acórdão do Tribunal de Justiça estadual quanto à incidência de ICMS e ao levantamento do depósito pelo Estado de Minas Gerais" (STJ, 1ª Turma, REsp 658.626/MG, rel. Min. Denise Arruda, DJe 22-9-2008).

"Tributário. Agravo de instrumento. Art. 544 do CPC. ICMS. Serviços prestados pelos provedores de acesso a Internet. Modalidade banda larga. Serviço de valor adicionado. Art. 61, § 1º, da Lei n. 9.472/97. Não incidência. Posicionamento da primeira seção. Julgamento dos EREsp 456.650/PR. Recurso desprovido. 1. A Lei n. 9.472/97, que dispõe sobre a organização dos serviços de telecomunicações, em seu art. 61, caput, prevê: 'Serviço de valor adicionado é a atividade que acrescenta, a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações'. 2. O serviço de conexão à Internet, por si só, não possibilita a emissão, transmissão ou recepção de informações, deixando de enquadrar-se, por isso, no conceito de serviço comunicacional. Para ter acesso à Internet, o usuário deve conectar-se a um sistema de telefonia ou outro meio eletrônico, este sim, em condições de prestar o serviço de comunicação, ficando sujeito à incidência do ICMS. O provedor, portanto, precisa de uma terceira pessoa que efetue esse serviço, servindo como canal físico, para que, desse modo, fique estabelecido o vínculo comunicacional entre o usuário e a Internet. É esse canal físico (empresa de telefonia ou outro meio comunicacional) o verdadeiro prestador de serviço de comunicação, pois é ele quem efetua a transmissão, emissão e recepção de mensagens. 3. A atividade exercida pelo provedor de acesso à Internet configura na realidade, um 'serviço de valor adicionado': pois aproveita um meio físico de comunicação preexistente, a ele acrescentando elementos que agilizam o fenômeno comu-

nicacional. 4. A Lei n. 9.472/97 (Lei Geral de Telecomunicações) ao definir, no art. 61, o que é o serviço de valor adicionado, registra: 'Serviço de valor adicionado a atividade que acrescenta, a um serviço de telecomunicação, que lhe dá suporte e com o qual não se confunde, novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de mensagens'. E dessa menção ao direito positivo já se percebe que o serviço de valor adicionado, embora dê suporte a um serviço de comunicação (telecomunicação), com ele não se confunde. 5. A função do provedor de acesso à Internet não é efetuar a comunicação, mas apenas facilitar o serviço comunicação prestado por outrem. 6. Aliás, nesse sentido posicionou-se o Tribunal: 'O serviço prestado pelo provedor de acesso à Internet não se caracteriza como serviço de telecomunicação, porque não necessita de autorização, permissão ou concessão da União' (art. 21, XI, da Constituição Federal). Tampouco oferece prestações onerosas de serviços de comunicação (art. 2º, III, da LC n. 87/96), de forma a incidir o ICMS, porque não fornece as condições e meios para que a comunicação ocorra, sendo um simples usuário dos serviços prestados pelas empresas de telecomunicações. Trata-se, portanto, de mero serviço de valor adicionado, uma vez que o prestador se utiliza da rede de telecomunicações que lhe dá suporte para viabilizar o acesso do usuário final à Internet, por meio de uma linha telefônica, atuando como intermediário entre o usuário final e a Internet. Utiliza-se, nesse sentido, de uma infraestrutura de telecomunicações preexistente, acrescentando ao usuário novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações (art. 61 da Lei Geral de Telecomunicações). 'O provimento de acesso não pode ser enquadrado (...) como um serviço de comunicação, pois não atende aos requisitos mínimos que, técnica e legalmente, são exigidos para tanto, ou seja, o serviço de conexão à Internet não pode executar as atividades necessárias e suficientes para resultarem na emissão, na transmissão, ou na recepção de sinais de telecomunicação. Nos moldes regulamentares, é um serviço de valor adicionado, pois aproveita uma rede de comunicação em funcionamento e agrega mecanismos adequados ao trato do armazenamento, movimentação e recuperação de informações' (José Maria de Oliveira, *apud* Hugo de Brito Machado, in 'Tributação na Internet', Coordenador: Ives Gandra da Silva Martins, Ed. Revista dos Tribunais, São Paulo, 2001, p. 89) (RESP 456.650/PR, Ministro Franciulli Netto). 7. Consectariamente, o serviço de valor adicionado, embora dê suporte a um serviço de comunicação (telecomunicação), com ele não se confunde, pois seu objetivo não é a transmissão, emissão ou recepção de mensagens, o que, nos termos do § 1º, do art. 60, desse diploma legal, é atribuição do serviço de telecomunicação. 8. Destarte, a função do provedor de acesso à Internet não é efetuar a comunicação, mas apenas facilitar o serviço comunicação prestado por outrem, no caso, a companhia telefônica, aproveitando uma rede de comunicação em funcionamento e a ela agregando mecanismos adequados ao trato do armazenamento, movimentação e recuperação de informações. 9. O ser-

viço de provedor de acesso à Internet não enseja a tributação pelo ICMS, considerando a sua distinção em relação aos serviços de telecomunicações, subsumindo-se à hipótese de incidência do ISS, por tratar-se de serviços de qualquer natureza. 10. Registre-se, ainda, que a lei o considera 'serviço', ao passo que, o enquadramento na exação do ICMS implicaria analogia instituidora de tributo, vedado pelo art. 108, § 1º, do CTN. 11. Deveras, é cediço que a analogia é o primeiro instrumento de integração da legislação tributária, consoante dispõe o art. 108, § 1º, do CTN. A analogia é utilizada para preencher as lacunas da norma jurídica positiva, ampliando-se a lei a casos semelhantes. Sua aplicação, *in casu*, desmereceria aplausos, uma vez que a inclusão dos serviços de Internet no ICMS invadiria, inexoravelmente, o terreno do princípio da legalidade ou da reserva legal que, em sede de direito tributário, preconiza que o tributo só pode ser criado ou aumentado por lei. 12. Consectariamente, a cobrança de ICMS sobre serviços prestados pelo provedor de acesso à Internet violaria o princípio da tipicidade tributária, segundo o qual o tributo só pode ser exigido quando todos os elementos da norma jurídica — hipótese de incidência, sujeito ativo e passivo, base de cálculo e alíquotas — estão contidos na lei. 13. No julgamento dos EREsp 456.650/PR, em 11 de maio de 2005, a Primeira Seção, por maioria de votos, negou provimento aos embargos de divergência, fazendo prevalecer o entendimento da Segunda Turma, no sentido de ser indevida a incidência de ICMS sobre os serviços prestados pelos provedores de acesso à Internet, sob o fundamento de que esses prestam serviços de valor adicionado, nos termos do art. 61, § 1º, da Lei n. 9.472/97, apenas liberando espaço virtual para comunicação. 14. Agravo Regimental desprovido" (STJ, 1ª Turma, AgRg nos EDcl no Ag 883.278/RJ, rel. Min. Luiz Fux, *DJe* 5-5-2008).

PROVA DA DECLARAÇÃO DE IR VIA INTERNET

"Penal. Art. 1º, I, da Lei n. 8.137/90. Prestação de declarações falsas de imposto de renda. Supressão de tributos. Materialidade e autoria. Dolo. 1. Comprovada a autoria pelas cópias do Contrato Social da empresa, bem como pelos depoimentos de ambos os réus, onde admitem que exercem, conjuntamente, a administração da sociedade. 2. As declarações de imposto de renda, tanto para pessoa física como para pessoa jurídica, enviadas por meio eletrônico, através da *web*, prescindem da assinatura do declarante. A prova material do recebimento se dá através de um recibo eletrônico, enviado pela Receita para o computador que transmitiu a declaração. Tal recibo é aceito perfeitamente como prova do envio da declaração. No caso dos autos, o recibo não veio aos autos juntamente com a declaração, mas a prova testemunhal referida é suficiente para suprir a sua ausência, até porque os réus em nenhum momento negam o envio da declaração por meio digital, sendo,

portanto, fato incontroverso. 3. O dolo é genérico e inerente ao tipo penal do art. 1º, I, da Lei n. 8.137/90, que não prevê a modalidade culposa. 4. 'A consumação do crime tipificado no art. 1º, *caput*, ocorre com a realização do resultado, consistente na redução ou supressão do tributo ou da contribuição social (evasão proporcionada pela prática da conduta fraudulenta anterior)'. (Andreas Eisele, em 'Crimes Contra a Ordem Tributária', 2. ed., Dialética, fl. 146). 5. Apelação improvida" (TRF4, 7ª Turma, ACR 2001.71.08.005548-2, rel. José Luiz Borges Germano da Silva, DJ 29-10-2003).

VALIDADE DE NOTIFICAÇÃO VIA INTERNET. TRIBUTÁRIO

*"Tributário e processual civil. Mandado de segurança. Manutenção no REFIS de empresa excluída por ofensa ao art. 5º, II, da Lei n. 9.964/2000. Procedimento sumário e/ou virtual. Violação dos princípios do contraditório, ampla defesa, publicidade e motivação não caracterizada. Benefício/favor fiscal se interpreta restritivamente. Inobservância de exigências. CND. 1. O REFIS (Lei n. 9.964/2000) é tipo de moratória mediante adesão voluntária via Internet que implica confissão irrevogável e irreatável dos débitos consolidados, sujeito às condições preestabelecidas e conhecidas, incluídos os casos de exclusão pelo não cumprimento de qualquer delas. 2. Tal programa é regido especificamente pela Lei n. 9.964/2000, afastando-se, em consequência, a aplicação da norma subsidiária (Lei n. 9.784/99), porquanto, nos termos do art. 69 da Lei n. 9.784/99, 'os processos administrativos específicos continuarão a reger-se por lei própria, aplicando-se-lhes apenas subsidiariamente os preceitos desta Lei'. 3. Matéria pacificada no âmbito do STJ, por meio da Súmula 355: 'É válida a notificação do ato de exclusão do Programa de Recuperação Fiscal REFIS pelo Diário Oficial ou pela Internet'. 4. Legalidade do procedimento sumário/virtual de exclusão do REFIS, verificado o descumprimento de condições estabelecidas pela lei de regência (Lei n. 9.964/2000). 5. Não merece prosperar a pretensão de se obter a reinclusão no REFIS, uma vez que os fundamentos do ato de exclusão são bem mais amplos, discutindo-se, inclusive, a existência de outros débitos posteriores ao REFIS, como bem observou o Juiz *a quo*. 6. A exclusão do REFIS configura motivo impeditivo para a não concessão da certidão Positiva com efeitos de negativa. 7. Apelação não provida. Sentença mantida" (TRF01, 7ª Turma AMS 0000665-74.2008.4.01.3814/MG, rel. Des. Federal Reynaldo Fonseca, e-DJF1 p. 313 de 14-5-2010).*

"REFIS. Exclusão. Notificação pessoal. Desnecessidade. Recolhimento das parcelas pelo regime do simples. Impossibilidade. 1. Não obstante os pagamentos efetuados pela parte autora no parcelamento efetuado, o fato é que de modo algum poderia deixar

de pagar os impostos e contribuições posteriores à data de sua opção pelo REFIS. Isso porque, tendo sido excluída do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e das Empresas de Pequeno Porte — SIMPLES, em 9-1-1999, pelo Ato Declaratório n. 0177800 da Secretaria da Receita Federal, do qual foi notificada por AR em 26-1-1999, deveria ter retornado ao pagamento de suas obrigações fiscais, pela forma geral, que não a simplificada. Correta, portanto, a sua exclusão do REFIS, pela incidência da parte final do inciso II do art. 5º da Lei n. 9.964/00. 2. Quanto à forma de exclusão do REFIS, este Tribunal vem sufragando o entendimento de que a notificação via Internet é viável, sem implicar em violação à lei ou à Carta Constitucional e sendo, ademais, compatível com as regras de adesão ao plano, quanto à simplicidade dos procedimentos" (TRF4, 1ª Turma, AC 2002.71.00.037265-2, rel. Maria Lúcia Luz Leiria, DJ 13-7-2005).

"Programa de recuperação fiscal. REFIS. Exclusão. Ausência de notificação pessoal. Notificação por meio do diário oficial e da Internet. Possibilidade. REsp 1.046.376/DF. Matéria julgada sob o regime do art. 543-C do CPC. 1. A controvérsia dos autos reside em saber se é legítima a exclusão do contribuinte que aderiu ao REFIS e tornou-se inadimplente, mediante publicação da Portaria no Diário Oficial da União e na rede mundial de computadores — Internet —, ou se seria imprescindível a notificação pessoal. 2. A Primeira Seção do STJ, no julgamento do recurso repetitivo REsp 1.046.376/DF, em 11-2-2009, reafirmou entendimento segundo o qual é legítima a exclusão do contribuinte que aderiu ao REFIS e tornou-se inadimplente, mediante publicação na rede mundial de computadores — Internet. 3. Aplica-se ao caso a multa do art. 557, § 2º, do CPC no percentual de 10% (dez por cento) sobre o valor da causa, por questionamento de matéria já decidida em recurso repetitivo. Agravo regimental improvido" (STJ, 2ª Turma, AgRg no REsp 1.205.170/DF, rel. Min. Humberto Martins, j. 16-8-2011, DJe 22-8-2011).

"Processual civil. FGTS. Transação extrajudicial. Lei Complementar n. 110/2001. Decreto n. 3.913/2001. Adesão por meio eletrônico. Possibilidade. O art. 4º da LC n. 110, de 29-6-2001, possibilitou a transação entre as partes no recebimento dos valores relativos ao FGTS, viabilizada a adesão ao referido acordo por meios magnéticos ou eletrônicos, inclusive mediante teleprocessamento, a teor do que dispõe o § 1º do art. 3º do Decreto n. 3.913, de 11 de setembro de 2001. Validade e eficácia do ato reconhecidas. Precedentes do STJ e da Primeira Seção desta Corte. Recurso da parte autora desprovido. (TJSP, 2ª Turma, 2009.61.20.006187-6, rel. Des. Peixoto Junior, j. 26-4-2011).

"Tributário. Mandado de segurança coletivo. Legitimidade passiva da autoridade impetrada. Portarias MPAS n. 375/2001 e 2.744/2001. Recolhimento das contribuições

sociais arrecadadas pelo INSS exclusivamente por meio de débito em conta comandado por intermédio da rede Internet ou de aplicativos eletrônicos disponibilizados pelos bancos. *Legalidade*. 1. Inicialmente, verifica-se a legitimidade passiva da autoridade impetrada, uma vez que o Diretor Superintendente do Instituto Nacional do Seguro Social — INSS — ocupa a posição mais elevada da estrutura hierárquica da autarquia nos Estado do Rio de Janeiro, e, portanto, é autoridade que tem o poder funcional para executar e exigir dos associados da impetrante o cumprimento da portaria questionada. 2. A Portaria do Ministério da Previdência e Assistência Social n. 375, de 24 de janeiro de 2001, determinou, nos arts. 1º e 2º, que, a partir de fevereiro de 2001, respectivamente, os recolhimentos das contribuições sociais arrecadadas pelo Instituto Nacional do Seguro Social (INSS) de empresas deverão ser efetuados, exclusivamente, mediante débito em conta comandado por meio de rede de Internet ou por aplicativos eletrônicos disponibilizados pelos bancos; e que os bancos contratados pelo INSS para a execução dos serviços de arrecadação deverão dispor de sistemas que permitam o recolhimento das contribuições sociais pelos meios mencionados anteriormente, ressaltando que, excepcionalmente, até 30 de junho de 2001, a rede bancária contratada poderá proceder ao recolhimento em guichê de caixa, data que foi prorrogada para 30 de novembro de 2001 pela Portaria MPAS n. 2.744, de 27 de julho de 2001. 3. A referida portaria não ofende o princípio da legalidade, porquanto o regramento da forma, do mecanismo de arrecadação, enquanto obrigação tributária acessória, por não afetar a configuração da obrigação tributária principal, ou seja, a identificação do sujeito passivo, a definição da hipótese de incidência e a quantificação do dever jurídico tributário mediante o estabelecimento das respectivas alíquota e base de cálculo, não se sujeita ao princípio da legalidade. Ao contrário, o CTN insere a sua disciplina no poder regulamentar da Administração Pública, permitindo, no art. 96 conjugado com o § 2º do art. 113, que atos normativos complementares, como o decreto e a portaria, venham dispor a respeito. 4. Ademais, ainda que seja possível a existência de pequenas empresas sem o apropriado acesso à Internet, a portaria em apreciação obriga os bancos a disponibilizar aplicativos eletrônicos em suas agências para tal finalidade, de sorte que o ato normativo impugnado não onera os contribuintes que não tenham conta bancária ou acesso próprio à Internet com gastos exagerados e desproporcionais, nem obsta o recolhimento do tributo. 5. Remessa necessária e apelação providas” (REsp-RJ 2002.51.01.014349-5, 3ª Turma Especializada, rel. Des. Federal Luiz Mattos, j. 21-10-2008, DJU 31-10-2008, p. 174).

“Tributário. ISS. Provedor de internet. Não incidência. Ausência de previsão na lista do Decreto n. 406/68. 1. O serviço de acesso à Internet não consta da lista anexa do Decreto n. 406/68, não podendo sofrer a incidência do ISS. Precedentes.

2. Agravo regimental não provido” (STJ, 2ª Turma, AgRg no REsp 1.214.452/SP, rel. Min. Castro Meira, j. 28-6-2011, DJe 1º-7-2011).

“*Recurso especial. Negativa de prestação jurisdicional. Não ocorrência. Execução por quantia certa. Penhora online. Sistema BACEN-JUD. Pedido realizado após vigência da Lei n. 11.382/2006. Exaurimento das diligências para a localização de bens passíveis de penhora. Desnecessidade. Escólio jurisprudencial. Recurso especial provido.* I — Não há omissão no aresto *a quo*, no qual analisou as matérias que, na sua compreensão, foram relevantes para solução da controvérsia. II — Com a edição da Lei n. 11.382/2006, responsável pela inserção do art. 655-A, no Código de Processo Civil, conferiu-se ao Poder Judiciário mecanismo compatível com a modernidade tecnológica, notadamente, a Internet, por meio da qual se determina, por meio do denominado sistema BACEN-JUD, a ordem de bloqueio de contas ou investimentos dos devedores. III — Contudo, para melhor aplicação do novel diploma legal, a jurisprudência desta Corte Superior estabeleceu dois entendimentos, tendo como norte a vigência da Lei n. 11.382/2006. Nesse contexto, se o pedido de penhora *online* for requerido antes da vigência da Lei n. 11.382/2006, entende-se que tal medida é cabível apenas quando o exequente comprovar que exauriu as vias extrajudiciais de busca dos bens do executado. Todavia, se o pedido de penhora *online* for realizado após a vigência da supracitada lei, a orientação assente é no sentido de que essa penhora não exige mais a comprovação de esgotamento de vias extrajudiciais de busca de bens a serem penhorados. Na espécie, o pedido de penhora *online* realizou-se na vigência do novo diploma legal. IV — Recurso especial provido” (STJ, 3ª Turma, REsp 1.159.807/ES, rel. Min. Massami Uyeda, j. 16-6-2011, DJe 29-6-2011).

“*Indenização. Danos morais e materiais. Prestação de serviços. Telefonia fixa e Internet. Interrupção na prestação dos serviços, por falha da fornecedora. Relação de consumo caracterizada. Ônus da prova que incumbia à ré, acerca da regular prestação dos serviços, o que não ocorreu. Dever de indenizar o consumidor pelos danos causados. Danos materiais comprovados documentalmente. Danos morais decorrentes da falha na prestação dos serviços. Ação procedente. Sentença mantida, nos termos do art. 252 do Regimento Interno do TJSP. Apelo improvido*” (TJSP, Apelação 0035049-38.2010.8.26.0007, rel. Des. Salles Vieira, j. 10-11-2011).

RESPONSABILIDADE EXCLUSIVA DO USUÁRIO POR ATO ILÍCITO PRATICADO POR MEIO DO SITE DE RELACIONAMENTO "ORKUT"

Comentários:

Por tratar-se de provedor de conteúdo, é difícil afirmarmos que não há responsabilidade das redes sociais pelo conteúdo que disponibiliza em seu espaço virtual. E é justamente para afastar sua responsabilidade perante terceiros que provedores de conteúdo devem se resguardar para poder identificar o responsável pelo ato ilícito perpetrado por meio de seu sistema, sob pena de ser responsabilizado por aquele ato. Certamente não pode haver censura prévia, *vide* a garantia da liberdade de expressão. Mas, a partir da ciência do fato ilícito ou antiético, deve o provedor da página em que o conteúdo está diligenciar de forma célere para não caracterizar negligência nem conivência (coautoria).

De fato, a única forma de se manter isento nessa relação é por meio da guarda dos registros de acesso do usuário de seus serviços. Isso, em regra, tem isentado os provedores de conteúdo da responsabilidade por ato ilícito.

No tocante aos incidentes de *cyberbullying*, por envolver em sua maioria menores de idade, é fundamental agir rápido para retirada do conteúdo ofensivo e vexatório do ar. E os responsáveis legais respondem pela má conduta, pela indenização da vítima.

"Relação de consumo. Responsabilidade civil. Ação de obrigação de fazer. Danos morais. Internet. Provedor de acesso. Legitimidade. Google. Sítio de relacionamento (Orkut). Criação de perfil falso. Terceiro. Mensagens ofensivas a integrantes da comunidade a que pertence o autor. Antecipação de tutela. Retirada do sítio falso. Indenização. Descabimento. Preliminar de ilegitimidade passiva *ad causam* que se acolhe apenas em relação ao corréu, M.P.M. e L. Ltda., o qual se limita a somente prestar serviços de proteção à marca 'Google' como agente de propriedade industrial. O Google Brasil Internet Ltda., que faz parte do mesmo grupo empresarial da Google, Inc., é parte legítima para figurar no polo passivo da ação indenizatória que tem como fundamento ato ilícito praticado nos domínios do sítio eletrônico denominado Orkut, de que é proprietário. Através desse serviço, os usuários criam páginas pessoais ('perfis') a partir das quais se comunicam com os demais e participam de diversas comunidades. Ainda que o serviço, que é objeto da ação, seja prestado envolvendo provedores de acesso à Internet ou responsáveis por

sites de relacionamento e os respectivos usuários, não sendo direta ou indiretamente remunerado, aplica-se a legislação consumerista. Aquele que é prejudicado por defeito ou falha na prestação de serviços, tendo ou não relação jurídica direta com o fornecedor, qualifica-se como consumidor (art. 17 da Lei n. 8.078/90). Fato de terceiro. As páginas de relacionamento são marcadas pelo dinamismo, pelo amplo e irrestrito acesso a qualquer indivíduo em qualquer parte do mundo e, consequentemente, pela ausência de qualquer formalidade prévia. Página fraudada por terceiro de molde a conter informações ofensivas ao usuário ou a integrantes da mesma comunidade no Orkut, como se as mesmas tivessem sido criadas e/ou remetidas por este. Circunstância *sui generis* a envolver nova tecnologia e novas relações interpessoais. A possibilidade de identificar o usuário que enviou as mensagens falsas em nome do autor, através do IP (*Internet Protocol*), nem sempre é suficiente para identificar quem seria o real ofensor. Lado outro, inexistindo dever legal ou contratual de monitoramento prévio ou fiscalização antecipada do conteúdo das páginas pessoais, de modo a controlar esse conteúdo e impedir a prática de atos ilícitos (como a adulteração de dados), ou inquinados (como a irrogação de injúrias, calúnias e difamações), por outros usuários ou terceiros, afasta o dever de indenizar. Sem a comprovação do defeito do serviço perde-se um dos requisitos imprescindíveis para a caracterização da responsabilidade civil objetiva (art. 14 da citada Lei n. 8.078/90), sendo certo que a responsabilidade do provedor de acesso e responsável pelo site de relacionamento se circunscreve à disponibilização da tecnologia que permite o acesso à WEB. Harmonização do direito à imagem com o preceito que assegura a livre manifestação do pensamento e da informação vedando, entretanto, o anonimato nas livres manifestações de pensamento (art. 5º, inc. IV, IX, X e XIV da CRFB/88). Provedor de hospedagem que não está obrigado a fiscalizar, nem realizar qualquer censura prévia ou genérica (o que avilta, ademais, os princípios democráticos insculpidos na Constituição vigente), sobre o conteúdo inserido pelos usuários. Diante da impossibilidade de fiscalizar todas as páginas criadas, e ainda, observando a garantia fundamental do livre pensamento, se torna impossível a exclusão do nome da agravada, sem que esta identifique as respectivas URL (Localizador de Recursos Universal). Ausência de conduta culposa pelo réu, pois não restou evidenciada a negligência, a imprudência ou imperícia. Sentença mantida. Recurso a que se nega provimento" (TJRJ, Agravo de Instrumento 0374854-06.2008.8.19.0001 (2009.001.69800), rel. Mario Assis Gonçalves, j. 22-6-2010).

"Ação de indenização. Dano moral. Orkut. Rede social. Sítio de relacionamento. Internet. Provedor de serviços de informações. Responsabilidade por fato do serviço. Direito do consumidor. Responsabilidade objetiva. Usuário vítima do evento. Ofensas de cunho moral. Expressão 'fazendo a fila andar'. Quantum. (...). A relação entre os provedores e usuários da Internet é regida pelas normas do Código de Defesa do Consumidor. Os provedores se enquadram como fornecedores de serviços (...). A

expressão 'fazendo a fila andar', aposta por usuário inidôneo na denominação do perfil pessoal da usuária atinge a sua honra subjetiva. A expressão 'fazer a fila andar', no jargão popular, significa sucessão de parceiros amorosos, denotando promiscuidade por meio de relacionamento sexual não monogâmico, ou seja, com muitos parceiros diferentes (...)" (TJMG, Recurso 1.0145.08.471404-0/001(1), rel. Cabral da Silva, j. 3-8-2010).

"Ação de indenização. Dano moral. Ofensas e acusações em site de relacionamentos — Orkut. Prova nos autos que demonstra que a ré se utilizou do site de relacionamentos Orkut para ofender, proferir acusações e denegrir a imagem da autora, perante todas as pessoas que têm acesso ao conteúdo das mensagens de cunho manifestamente ofensivo. Violação a direito de personalidade, de molde a atingir a honra e imagem da parte autora. Danos morais configurados. Redução do quantum indenizatório. Sentença parcialmente reformada. Recurso parcialmente provido" (TJRS, Recurso Cível 71002312858, rel. Eduardo Kraemer, j. 26-3-2010).

"Danos morais. Indenização. Criação de comunidade por ex-aluno contendo ofensas e injúria a colégio em sitio de relacionamentos 'Orkut'. Comprovada conduta ilícita. Reconvenção improcedente. Sanção regularmente aplicada. Sentença mantida. Recurso não provido. Danos morais. Provedora de serviços que apenas disponibiliza espaço para armazenamento de páginas dos usuários. Ausência de responsabilidade. Impossibilidade de monitoramento. Notificação judicial efetuada após exclusão da comunidade. Inexistência de notificação extrajudicial anterior. Ausência de descumprimento da ordem liminar ou de omissão. Culpa não demonstrada. Sentença reformada. Recurso provido" (TJSP, Apelação 578.863-4/3-00, rel. Elcio Trujillo, j. 18-2-2009).

"Ação indenizatória. Rito sumário. Ofensas inseridas por terceiros em páginas do Orkut. Responsabilidade pelo dano moral. Sentença julgando improcedente o pedido. Reforma. Cabimento da indenização, já que a Constituição Federal proíbe o anonimato e a Google não identificou, tampouco denunciou a lide ou chamou ao processo os usuários responsáveis pelos atos. Art. 5º, IV e V. Fixação em R\$ 25.000,00, sendo R\$ 15.000,00, para a segunda autora, e R\$ 10.000,00 para a outra. Ação que se julga procedente. Provimento do Recurso" (TJRJ, Apelação 2008.001.56760, rel. Des. Otavio Rodrigues, j. 3-12-2008).

"Indenização. Danos morais. Pessoa jurídica é titular de bens extrapatrimoniais e pode ter sua reputação lesada. Possibilidade de reconhecer o dano

moral para a pessoa jurídica, quando lesado seu nome ou honra subjetiva. Aluno de academia insatisfeito tece ofensas e injúria por meio do *site* de relacionamentos orkut.com. *Site* público. As críticas ao serviço prestado pela autora extrapolam o limite do aceitável. Ofensas diretas sem pertinência com fatos concretos. Lesão à imagem da academia perante terceiros. *Quantum* indenizatório bem fixado. Ônus de sucumbência adequados. Ação procedente. Recurso não provido" (TJSP, Apelação Cível 529 776-4/2-00, rel. Francisco Loureiro, j. 13-11-2008).

"Danos morais. Ofensas proferidas contra a empresa-ré e sua ombudsman através de página na Internet. Repercussão inimaginável do meio. Indenização devida. Sentença de procedência mantida. Recurso improvido" (TJSP, rel. Des. Caetano Lagrasta, j. 13-11-2008).

"(...) Observa-se que vários recados foram deixados no site de relacionamentos denominado 'Orkut' e, ao contrário do que sustenta, são indicativos de que estava subtraindo numerário da empresa, em conluio com o fiscal G. (...) Isso porque além de o próprio obreiro noticiar em sua página do site de relacionamentos do 'Orkut', às escancaras, suas atividades ilegais, denominando a si mesmo de 'corrupto' (fls.35), o que por si só afastaria a pretensão por danos morais, não há provas de que a reclamada tenha informado à imprensa o ocorrido (...) (TRT15, RO/00392-2007-121-15-00-9, rel. Edna Pedroso Romanini, publ. 4-7-2008).

"Apelação cível. Ação de indenização cumulada com condenatória a obrigação de fazer. Internet. Google. Orkut. Criação de perfil falsamente atribuído ao autor. Provedor de hospedagem. Responsabilidade objetiva. Aplicação do Código de Defesa do Consumidor. Responsabilidade inerente à natureza da atividade desenvolvida. Nomeação à autoria. Dever do réu. Danos morais convertidos em indenização por perdas e danos decorrentes da falta de nomeação. Recurso provido. 1 — O Google, responsável pelo site de relacionamentos denominado Orkut, está sujeito ao Código de Defesa do Consumidor nas relações com seus usuários. 2 — O Orkut é um provedor de serviço de Internet que se caracteriza pela hospedagem de páginas pessoais de usuários, possibilitando a troca de mensagens e a criação de comunidades, que ganham adeptos conforme interesses, ideias ou curiosidades comuns. (...) 4 — O Google responde de forma objetiva pelo provedor de hospedagem e pela confidencialidade dos dados dos seus usuários, mas não pelo conteúdo inserido em cada perfil individual. 5 — É impossível a retirada de conteúdo da rede sem a provoca-

ção da parte interessada, diante da inviabilidade técnica, fática e jurídica de o provedor de hospedagem varrer seus servidores à procura de um determinado tipo de informação. 6 — A criação de perfil falsamente atribuído ao Autor somente pode ser aferida pelo próprio ofendido, pois a eficiência dos mecanismos de filtragem de conteúdo inseridos no Orkut depende de indicação precisa da parte interessada. 7 — O Google possui meios adequados à identificação do usuário do Orkut que pratique eventual ilegalidade, promovendo o eficiente rastreamento dos usuários infratores, impedindo, assim, o anonimato, diligência razoável imputada a um provedor de conteúdo de Internet. 8 — O Google detém o perfil do Orkut em nome alheio, já que a propriedade da coisa (conteúdo do perfil) é do próprio usuário. 9 — Competia ao Google promover a nomeação à autoria do verdadeiro criador do perfil ofensivo ao Autor. A omissão, existente sentença de mérito, impõe ao Réu o dever indenizatório ao Autor. 10 — Recurso não provido — (TJMG, Apelação Cível 1.0024.10.045653-2/002 ou 0456532-68.2010.8.13.0024, j. 11-5-2011, publ. 18-5-2011).

“Apelação. Responsabilidade civil. Internet. Uso de imagem para fim depreciativo. Criação de flog — página pessoal para fotos na rede mundial de computadores. Responsabilidade dos genitores. Pátrio poder. Bullying. Ato ilícito. Dano moral in re ipsa. Ofensas aos chamados direitos de personalidade. Manutenção da indenização. Provedor de internet. Serviço disponibilizado. Comprovação de zelo. Ausência de responsabilidade pelo conteúdo. Ação. Retirada da página em tempo hábil. Preliminar afastada. Denúnciação da lide. Ausência de elementos. Apelo do autor da denúnciação da lide. I. Para restar configurada a denúnciação da lide, nos moldes do art. 70 do CPC, necessário elementos demonstrando vínculo de admissibilidade. Ausentes provas embasando o pedido realizado, não há falar em denúnciação da lide. Da responsabilidade do provedor de Internet. II. Provedores de Internet disponibilizam espaço para criação de páginas pessoais na rede mundial de computadores, as quais são utilizadas livremente pelos usuários. Contudo, havendo denúncia de conteúdo impróprio e/ou ofensivo à dignidade da pessoa humana, incumbe ao prestador de serviços averiguar e retirar com brevidade a página se presente elementos de caráter ofensivo. III. Hipótese em que o provedor excluiu a página denunciada do ar depois de transcorrida semana, uma vez ser analisado assunto exposto, bem como necessário certo tempo para o rastreamento da origem das ofensas pessoais — PC do ofensor. Ausentes provas de desrespeito aos direitos previstos pelo CDC, não há falar em responsabilidade civil do provedor. Apelo da ré. Do dano moral. IV. A Doutrina moderna evoluiu para firmar entendimento acerca da responsabilidade civil do ofensor em

relação ao ofendido, haja vista desgaste do instituto proveniente da massificação das demandas judiciais. O dano deve representar ofensa aos chamados direitos de personalidade, como à imagem e à honra, de modo a desestabilizar psicologicamente o ofendido. V. A prática de bullying é ato ilícito, haja vista compreender a intenção de desestabilizar psicologicamente o ofendido, o qual resulta em abalo acima do razoável, respondendo o ofensor pela prática ilegal. VI. Aos pais incumbe o dever de guarda, orientação e zelo pelos filhos menores de idade, respondendo civilmente pelos ilícitos praticados, uma vez ser inerente ao pátrio poder, conforme inteligência do art. 932 do Código Civil. Hipótese em que o filho menor criou página na Internet com a finalidade de ofender colega de classe, atrelando fatos e imagens de caráter exclusivamente pejorativo. VII. Incontroversa ofensa aos chamados direitos de personalidade do autor, como à imagem e à honra, restando, ao responsável, o dever de indenizar o ofendido pelo dano moral causado, o qual, no caso, tem natureza in re ipsa. VIII. Quantum reparatório serve de meio coercitivo/educativo ao ofensor, de modo a desestimular práticas reiteradas de ilícitos civis. Manutenção do valor reparatório é medida que se impõe, porquanto harmônico com caráter punitivo/pedagógico comumente adotado pela Câmara em situações análogas. Apelos desprovidos — (TJRS, 6ª Câmara Cível, Apelação Cível 70031750094, rel. Liege Puricelli Pires, j. 30-6-2010).

PROVA. DOCUMENTO EXTRAÍDO DA INTERNET. VALIDADE

“Convenção coletiva. Cópia. Validade. Tratando-se de documento comum às partes, e considerando a inexistência de impugnação aos seus termos, válida a juntada de convenção coletiva em cópia obtida por meio da Internet. Aplicação da Orientação Jurisprudencial n. 36, da SBDI-1, do C. TST. Diferenças de horas extras. Intervalo. Feriados. Admitida, já no libelo, a anotação da jornada cumprida nos cartões de ponto, exceção feita ao intervalo, prevalecem as assinalações constantes de tais documentos, trazidos aos autos pela parte contrária. Mais ainda, constatada por meio da análise da prova documental o pagamento das horas em sobejo, tidas como tais as excedentes ao limite previsto em norma coletiva, incumbia ao reclamante demonstrar eficazmente as dissensões alegadas, bem assim a fruição parcial do intervalo. Não se desvencilhando de forma satisfatória dessa obrigação, indevido o pagamento das diferenças pleiteadas. Feriados. Conteúdo documental em harmonia com o cálculo por amostragem oferecido, evidenciando o trabalho prestado em feriado e a inexistência de

compensação ou pagamento do adicional correspondente previsto em instrumento coletivo, autoriza a manutenção da condenação correspondente. *Adicional noturno. Prorrogação da jornada.* A prorrogação da jornada noturna deve ser considerada como hora noturna, com observância da redução prevista no art. 73, § 1º, da CLT para o cálculo das horas extras e pagamento de adicional noturno. Aplicação da Súmula n. 60, item II, do C.TST. *Honorários advocatícios.* O consenso manifestado pelo Tribunal Superior do Trabalho é o de que os honorários advocatícios, nesta Justiça Especializada, somente são devidos na ocorrência, simultânea, das hipóteses de gozo do benefício da justiça gratuita e da assistência do Sindicato da categoria profissional, para os trabalhadores que vençam até o dobro do salário mínimo ou declarem insuficiência econômica para demandar. Com ressalva de concepção diversa acata-se, por disciplina judiciária, esse posicionamento cristalizado nas Súmulas n. 219 e 329 e na Orientação Jurisprudencial n. 305 da SBDI-1, da mais alta Corte Trabalhista — (TRT02, RO 1297200622102000, rel. Des. Luiz Carlos Gomes Godói, DJ 23-9-2008).

INTERNET. SITE DE RELACIONAMENTO COMO MEIO DE PROVA

“Recurso ordinário em rito sumaríssimo. Testemunha que figura como amiga da parte no website de relacionamentos denominado Orkut. Acolhimento de contradita. Não se ignora que diversas ‘amizades’ travadas através da Internet jamais saem do campo da virtualidade. Entretanto, se a parte traz a Juízo uma testemunha que também figura como sua amiga no *website* de relacionamentos denominado Orkut, infere-se a existência de amizade íntima entre as mesmas eis que o relacionamento entre elas existente, além de obviamente não se restringir apenas ao campo virtual, certamente ultrapassou os limites laborais” (TRT, 2ª Região, RO em Rito sumaríssimo 02399200506302008, rel. Des. Ricardo Artur Costa e Trigueiros, DJ 29-9-2006).

PROPAGANDA ELEITORAL ANTECIPADA EM REDES SOCIAIS

“Representação. Propaganda eleitoral antecipada. Orkut. 1. Para rever o entendimento da Corte de origem, que concluiu estarem presentes os elementos caracterizadores da prática de propaganda eleitoral antecipada, em mensagens veiculadas no sítio de relacionamentos Orkut, seria necessário o revolvimento do

conjunto fático-probatório, o que não é possível na via eleita, a teor da Súmula n. 279 do egrégio Supremo Tribunal Federal. 2. As circunstâncias de que o sítio de relacionamentos teria acesso restrito e se limitaria a integrantes e usuários previamente cadastrados não afastam a infração legal, uma vez que as redes sociais na Internet constituem meios amplamente utilizados para divulgação de ideias e informações, razão pela qual não deve ser afastada a proibição da norma que veda a antecipação de campanha. 3. Não é cabível a aplicação do princípio da retroatividade da lei mais benéfica, porquanto as modificações trazidas pela Lei n. 12.034/2009 — que reduziu os valores de multa imposta em caso de propaganda eleitoral antecipada — não incidem em relação a fatos ocorridos antes do início de sua vigência. Agravo regimental a que se nega provimento. (10104 SP, rel. Min. Arnaldo Versiani Leite Soares, j. 19-8-2010, DJE 29-9-2010, p. 38).

PRÁTICA DE ATO ILÍCITO POR MENOR. RESPONSABILIDADE SOLIDÁRIA DOS PAIS NA REPARAÇÃO DE DANOS

Comentários:

A responsabilidade civil dos pais pelo ato ilícito praticado pelos filhos por meio da rede mundial de computadores é prevista no art. 932, I, do Código Civil. Dessa forma, qualquer que seja o efeito na esfera cível, do ato ilícito praticado pelo menor na rede mundial de computadores, aquele será suportado pelo seu responsável legal.

Por isso é tão importante a supervisão dos pais com relação à utilização das novas tecnologias pelos filhos, sob pena de responsabilização legal pelos seus efeitos. Segue abaixo decisões acerca da responsabilidade dos pais pelos efeitos civis dos atos ilicitamente praticados pelos filhos menores por meio da rede mundial de computadores.

“Indenizatória. Danos morais. Comunidade virtual. Divulgação, por menores, de mensagens depreciativas em relação a professor. Identificação. Linguagem chula e de baixo calão. Ameaças. Ilícito configurado. Ato infracional apurado. Cumprimento de medida socioeducativa. Responsabilidade dos pais. Negligência ao dever legal de vigilância. Os danos morais causados por divulgação, em comunidade virtual (Orkut) de mensagens depreciativas, denegrindo a imagem de professor (identificado por nome), mediante linguagem chula e de baixo calão, e com ameaças de depredação a seu patrimônio, devem ser ressarcidos. Incumbe aos pais, por dever legal de vigilância, a responsabilidade pelos ilícitos cometidos por filhos incapazes sob sua guarda” (TJRO, Apelação 100.007.2006.011349-2, rel. Des. Edenir Sebastião Albuquerque da Rosa, j. 20-8-2008).

“Apelação cível. Mandado de segurança. Expulsão de menor de instituição de ensino. Existência de procedimento administrativo. Contraditório e ampla defesa oportunizados. Demonstrando os autos a existência de regular procedimento administrativo, com contraditório e ampla defesa; ausente direito líquido e certo do impetrante a ser amparado por mandamos, correta a decisão que denegou a segurança. Apelo desprovido” (Segredo de Justiça) (TJRS, Apelação Cível 70021381850, rel. José Ataídes Siqueira Trindade, j. 1º-11-2007).

CARTA ROGATÓRIA. PROVA ELETRÔNICA PRODUZIDA NO BRASIL

Comentários:

A carta rogatória é o instrumento responsável pelo cumprimento de diligências requeridas por particulares através do Poder competente para tanto. Assim, nesse caso, houve o repasse de informações referentes à correspondência ameaçadora enviada a cidadão português, por meio de endereço de conexão brasileiro.

Dessa forma, foram repassados os dados cadastrais do responsável pelo envio de *e-mail* com conteúdo ameaçador. E, pelo cumprimento de seus objetivos, a carta foi devolvida ao país rogante para próximas diligências.

“Vistos etc. 1. O Tribunal de Instrução Criminal de Lisboa, República Portuguesa, solicita, mediante esta carta rogatória, que o representante legal da ‘Brasilvision Cine Vídeo Ltda.’ e MRAS informem a identidade completa do usuário do IP 200.222.76.21, no dia 9-10-2005, pelas 5:57:15 PM GMT. Narra o pedido rogatório que o referido usuário, utilizando-se do *e-mail* m(...)@hotmail.com, teria praticado crimes de ameaça e contra a honra de JMJM. Intimados previamente, via postal, os interessados informaram os dados do usuário (fls. 33-34). Determinada a intimação prévia da usuária indicada pela empresa interessada, JCM compareceu aos autos (fls. 89-97) para esclarecer que desconhece os fatos e as pessoas relacionadas ao caso, que nunca esteve em Portugal, bem como não criou o endereço de *e-mail* mencionado na comissão. Sustentou, assim, ter sido vítima da ação de um ‘hacker’ responsável por invadir seu computador e usurpar seus dados. O Ministério Público Federal opinou pela devolução dos autos à origem (fl. 101). 2. O objeto desta rogatória não atenta contra a soberania nacional ou a ordem pública. Os interessados, devidamente representados nos autos, prestaram todas as informações solicitadas pela Justiça rogante. 3. Ante o exposto, concedo o *exequatur* (art. 2º da Resolução n. 9/2005 deste Tribunal) e, tendo em vista o devido cumprimento da comissão rogatória, determino a devolução dos autos à Justiça rogante, por intermédio do Ministério Público Federal, autoridade central para o caso (art. 14, § 4º, Decreto n. 1.320/1994). Publique-se. Intimem-se” (STJ, Carta Rogatória n. 2.331 — Portugal, rel. Min. Barros Monteiro, publ. 4-12-2007).

Comentários:

A Lei n. 11.829/2008 alterou a redação do Estatuto da Criança e do Adolescente para considerar a armazenagem de conteúdo envolvendo menores também como crime, com pena de três a seis anos de reclusão e multa.

Dessa forma, o sujeito que armazena ou cria cenas de sexo explícito ou pornográficas envolvendo crianças comete crime de pedofilia e poderá ser punido por tal.

“Processo penal. Habeas corpus. Pretendida liberdade provisória. Prisão preventiva. Paciente acusado de condutas previstas nos arts. 241-A e 241-B da Lei n. 8.069/90, cometidas por meio da Internet. Necessidade da manutenção da prisão. Ordem denegada. 1. Habeas Corpus objetivando a concessão de liberdade provisória a homem preso em flagrante pela prática, em tese, dos crimes capitulados nos arts. 241-A e 241-B da Lei n. 8.069/90, via Internet. Pedido liminar indeferido. 2. O paciente disponibilizou conteúdo referente a atos de pedofilia por meio da Internet (usuário da rede Gigatribe, que compreende 900 mil outros), e no dia do cumprimento do mandado de busca e apreensão realizado em sua residência constatou-se o armazenamento de imagens de sexo explícito e pornografia infantojuvenil no disco rígido do computador pessoal dele. 3. A Polícia Federal, mediante autorização judicial, utilizou a identificação de um usuário brasileiro para ter acesso à comunidade virtual Gigatribe e, neste contexto, colheu provas de que o paciente, em tese, praticava os delitos. 4. Dentre as chamadas parafilias encontram-se manifestações sexualmente compulsivas como fetichismo, transvestismo fetichista, exibicionismo, voyeurismo, necrofilia e pedofilia. Os portadores dessas situações revelam padrão de comportamento caracterizado pela repetição como um quadro compulsivo. Essa compulsão acaba por trazer enorme dificuldade no controle da sua própria expressão significando um fator de maior propensão a condutas criminosas que podem vitimar pessoas que são a base das ‘fantasias’ que permeiam a respectiva parafilia. 5. Sucede que mesmo os comportamentos que podem anteceder as condutas violentas do portador dessa parafilia — como a excitação diante de simples imagens de práticas sexuais envolvendo pessoas pré-púberes — são repudiados em todo o mundo dito civilizado, e entre nós constituem-se em infrações penais graves. Nessa tipificação enxerga-se a presença do Direito Penal ‘preventivo’ — a exemplo do que antigamente se fazia na capitulação das chamadas ‘contravenções penais’ cujo objetivo era prevenir comportamentos danosos evolutivos para o ‘mal maior’ — que visa reprimir atos que possam consubstanciar manifestações da parafilia denominada de pedofilia, transtorno que pode evoluir para a situação muito mais séria de

abuso sexual infantil. 6. Necessidade de manutenção da prisão, até porque o paciente (estudante de pedagogia) trabalha numa ONG que cuida de crianças carentes; é certo que com essa singularidade profissional o paciente poderia com facilidade, em progressão criminosa, ‘evoluir’ da mera excitação sexual diante de imagens, à efetiva prática de libidinagem com indivíduos pré-púberes. 7. Ordem denegada” (TRF3, HC 2009.03.00.037603-7, rel. Johansom di Salvo, DJ 4-5-2010).

“Penal e processo penal. Recurso em sentido estrito. Divulgação/publicação, por meio da Internet, de pornografia infantil. Art. 241, ECA. Ausente prova de que a consumação do delito tenha ou devesse ter ocorrido no estrangeiro. Requisito da internacionalidade. Art. 109, V, da CF/88. Competência da justiça estadual. 1. Aos juízes federais compete processar e julgar os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente (Constituição Federal, art. 109, V). 2. O fato de o crime ser cometido através da ‘Internet’ não é suficiente para firmar a competência da Justiça Federal, sendo necessária a prova de que houve execução ou consumação do delito no exterior. 3. Sendo o crime iniciado no Brasil, sem prova da publicização em outro país, não é caso de crime à distância, cuja competência para processar e julgar é da justiça Estadual” (TRF4, 7ª Turma, Recurso em Sentido Estrito 0000178-76.2010.404.7201, rel. Sebastião Ogê Muniz, DJ 13-4-2010).

“Penal e processual penal. Recurso em sentido estrito. Publicação de pornografia envolvendo criança ou adolescente por meio da rede mundial de computadores (Internet). Art. 241 do Estatuto da Criança e do Adolescente (ECA). Competência da Justiça Federal. 1. Nos termos da jurisprudência do Superior Tribunal de Justiça, a consumação do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários. 2. Recurso em sentido estrito a que se dá provimento, declarando-se a Justiça Federal competente para o processamento e julgamento do feito” (TRF4, Recurso em Sentido Estrito 2009.72.01.002504-0, rel. Victor Luiz dos Santos Laus, DJ 24-2-2010).

“Penal e processo penal. Recurso criminal em sentido estrito. Divulgação/publicação, por meio da Internet, de fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente. Art. 241 do ECA (antiga redação). Competência. Art. 109, V, da CF/88. Inquérito policial em curso. Obtenção de e-mails sedia-

dos no exterior. Indícios suficientes da repercussão extraterritorial do delito. Manutenção do procedimento investigatório perante a justiça federal. 1. Para fins do disposto no art. 109, V, da CF/88, não havendo dúvidas de que o início da execução da conduta em tese perpetrada se deu no Brasil, mister restar demonstrada que a consumação da infração tenha ou devesse ter ocorrido no exterior. Tal assertiva não se modifica nas hipóteses em que a Internet é utilizada como meio para o cometimento de crimes: a prova (ou, pelo menos, indícios suficientes de prova) da execução do delito no Brasil e da sua consumação no exterior, ou vice-versa, mantém-se como pressuposto para que o feito seja processado e julgado pela Justiça Federal. Precedentes deste Tribunal e dos Tribunais Superiores. 2. Contudo, estando em curso inquérito policial, cujas investigações fazem referência a e-mails sediados no exterior, não há falar em exclusão, de plano, da repercussão extraterritorial do delito previsto no art. 241 do Estatuto da Criança e do Adolescente (divulgar ou publicar, pela Internet, fotografias pornográficas ou cenas de sexo explícito envolvendo crianças ou adolescentes), sobretudo porque ainda pendentes diversas diligências requeridas pelo *dominus litis* visando desvendar a autoria delitiva e as reais circunstâncias em que se deram os fatos” (TRF4, Recurso em Sentido Estrito 2009.71.02.003598-2, rel. Tadaaqui Hirose, DJ 9-2-2010).

“*Penal. Publicação de fotografias, contendo cenas de sexo explícito e pornográficas, envolvendo crianças e adolescentes. Art. 241 da Lei n. 8.069/90 (Estatuto da Criança e do Adolescente — ECA), em sua redação original, c/c art. 71 do Código Penal. Tipicidade da conduta, espelhada em duas práticas distintas, descritas na denúncia, a despeito da alteração introduzida, posteriormente, pela Lei n. 10.764/2003. Precedentes. Autoria e materialidade comprovadas. Dosimetria atenta ao disposto no art. 59 do Código Penal. Continuidade delitiva caracterizada. Sentença mantida.* I — Réu denunciado, como incurso na pena do art. 241 da Lei n. 8.069/90 (Estatuto da Criança e do Adolescente — ECA) — em sua redação original — c/c art. 71 do Código Penal, por ter (1) publicado fotos de pornografia infantil em ‘grupo de discussão’ do ‘Messenger Groups’, denominado ‘Thamansplace’, e (2) enviado um ‘e-mail’ para outra pessoa, contendo ‘links’ de acesso à pornografia infantil. II — A conduta imputada ao acusado, caracterizada por publicidade via Internet, espelhada nas duas práticas descritas na denúncia, é típica, diante da original redação do art. 241 da Lei n. 8.069/90, a despeito da alteração introduzida, posteriormente, pela Lei n. 10.764/2003, podendo ser autor do aludido crime qualquer pessoa, e não somente o proprietário de ‘site’ ou o provedor (Precedentes do STJ e do TRF/1ª Região: HC 2003.01.00.029307-6/MT, rel. Des. Federal Olindo Menezes, 3ª Turma do TRF/1ª Região, unânime, j. 21-10-2003, DJU de 31-10-2003, p. 36; HC 76.689/PB, rel. Min. Sepúlveda Pertence, 1ª Turma do STF, unânime, DJU 6-11-1998, p. 3; HC 84.561/PR, rel. Min. Joaquim Barbosa, 2ª Turma do STF,

unânime, DJU 26-11-2004, p. 31). III — Autoria e materialidade delitivas comprovadas, à saciedade, tornando inafastável a condenação imposta, pela prática de atos de verdadeira bestialidade humana, como se depreende das chocantes imagens constantes das fotografias colacionadas aos autos. IV — Dosimetria da pena que atende, criteriosamente, as circunstâncias judiciais do art. 59 do Código Penal, fazendo com que a pena-base fosse fixada em quantidade necessária e suficiente para a reprovação e prevenção do crime. V — Continuidade delitiva caracterizada pela prática de duas condutas absolutamente distintas, de forma continuada e materialmente comprovada, a ensejar o aumento da pena-base, pela aplicação da fração mínima (um sexto), prevista no art. 71 do Código Penal. VI — Apelação improvida” (TRF01, ACR 2003.36.00.014182-3/MT, rel. Assusete Magalhães, publ. 4-12-2009).

“*Apelação cível. Responsabilidade civil. E-mails relacionados com pornografia, pedofilia e crimes em série que abarrotaram o endereço eletrônico de usuário da Internet. Mensagens redirecionadas por outro provedor, em face de ato de terceiro. Nexos causal não configurado. Dever de indenizar do provedor que oferece serviços ‘e-grupos’ afastado.* 1. Segundo a teoria da asserção, a análise das condições da ação deve ser feita à luz das afirmações do autor em sua petição inicial. Ou seja, deve-se partir do pressuposto de que as afirmações do demandante em juízo são verdadeiras a fim de se verificar se as condições da ação estão presentes. Caso, no curso da demanda, se demonstre que as assertivas do autor não correspondem à realidade, há que se julgar improcedente o pedido, e não extinta a ação por ilegitimidade passiva. Caso concreto em que, pela narração da inicial, poderia haver responsabilidade do provedor Yahoo em relação a M. e M. Se esta versão dos fatos não corresponde à realidade, este é um aspecto que se compreende no mérito da demanda. Alegação de ilegitimidade ativa rejeitada. 2. Tendo o condão de interromper o curso do prazo prescricional a citação havida no processo cautelar, considerando que seu desfecho seria essencial para a propositura da ação de conhecimento, é de se afastar a alegação de prescrição da pretensão indenizatória. Ademais, contra o autor menor não correu prazo prescricional algum. 3. Restando comprovado nos autos que o endereço de e-mail do autor não foi incluído em qualquer dos grupos de discussão dos quais partiram as mensagens sobre pornografia, pedofilia e crimes em série que teriam lotado a sua caixa postal, já que quem estava cadastrado no grupo era a conta de terceiro e, por meio de um mecanismo de redirecionamento disponibilizado pelo provedor ‘mailbr.com.br’, foram automaticamente encaminhados ao endereço eletrônico do autor, não há responsabilidade do provedor Yahoo Brasil no evento danoso. Agravo retido desprovido. Apelo da ré provido. Apelo dos autores prejudicado” (TJRS, Apelação Cível 70030395107, rel. Marilene Bonzanini Bernardi, j. 28-10-2009).

“Criminal. REsp. Publicar cena de sexo explícito ou pornográfica envolvendo criança e adolescente via Internet. Embargos de declaração. Alínea ‘a’ do permissivo constitucional. Matéria debatida na instância a quo a despeito da não indicação do dispositivo legal. Prequestionamento implícito. Investigação. Ministério Público. Legitimidade. Súmula 234/STJ. Atipicidade da conduta. Análise dos termos publicar e divulgar. Identificação das crianças e adolescentes para a configuração do delito. Desnecessidade. ECA. Destinatários. Crianças e adolescentes como um todo. Suspensão condicional do processo. Prerrogativa do Ministério Público. Titular da ação penal pública. Recurso parcialmente provido. I. Hipótese em que o Ministério Público opôs embargos de declaração em face do acórdão proferido em sede de recurso de apelação, buscando o prequestionamento de dispositivos constitucionais e infraconstitucionais, com vistas à interposição de recursos nos Tribunais Superiores. II. O Tribunal a quo, no julgamento do recurso de apelação interposto pela defesa, tratou da matéria suscitada em embargos de declaração, sendo incabível a hipótese de violação do art. 619 do Código de Processo Penal. III. Ressalva de que o Superior Tribunal de Justiça já se manifestou no sentido de que em se tratando de recurso especial — interposto com fundamento na alínea ‘a’ do permissivo constitucional — admite-se a figura do prequestionamento em sua forma ‘implícita’, o que torna desnecessária a expressa menção do dispositivo legal tido por violado. Em contrapartida, torna-se imprescindível que a matéria em comento tenha sido objeto de discussão na instância a quo, configurando-se, assim, a existência do prequestionamento implícito. IV. Afasta-se a ideia da exclusividade da polícia judiciária para proceder às investigações de infrações penais, uma vez que o Ministério Público tem competência para tanto, e essa atuação não o impede dar início à ação penal correspondente. Súmula 234/STJ. V. Hipótese em que o Tribunal a quo afastou a tipicidade da conduta dos réus, sob o fundamento de que o ato de divulgar não é sinônimo de publicar, pois ‘nem todo aquele que divulga publica’, entendendo que os réus divulgavam o material, ‘de forma restrita, em comunicação pessoal, utilizando a Internet’, concluindo que não estariam, desta forma, publicando as imagens. VI. Se os recorridos trocaram fotos pornográficas envolvendo crianças e adolescentes através da Internet, resta caracterizada a conduta descrita no tipo penal previsto no art. 241 do Estatuto da Criança e do Adolescente, uma vez que permitiram a difusão da imagem para um número indeterminado de pessoas, tornando-as públicas, portanto. VII. Para a caracterização do disposto no art. 241 do Estatuto da Criança e do Adolescente, não se exige dano individual efetivo, bastando o potencial. Significa não se exigir que, em face da publicação, haja dano real à imagem, respeito à dignidade etc. de alguma criança ou adolescente, individualmente lesados. O tipo se contenta com o dano à imagem abstratamente considerada’. VIII. O Estatuto da Criança e do Adolescente garante a proteção integral a todas as crianças e adolescentes, acima de qualquer individualização. IX. A proposta de suspensão condicional do processo incumbe ao Ministério Público, titu-

lar da ação penal pública, sendo inviável sua propositura pelo julgador. X. Recurso parcialmente provido, para cassar o acórdão recorrido, dando-se prosseguimento à ação penal instaurada contra os réus” (STJ, REsp 617.221/RJ, rel. Min. Gilson Dipp, DJ 9-2-2005).

“Conflito negativo de competência. Processual penal. Publicação de pornografia envolvendo criança ou adolescente através da rede mundial de computadores. Art. 241 do Estatuto da Criança e do Adolescente. Competência territorial. Consumação do ilícito. Local de onde emanaram as imagens pedófilo-pornográficas. 1 — A consumação do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários. 2 — Conflito conhecido para declarar competente o Juízo da Vara Federal Criminal da Seção Judiciária de Santa Catarina” (STJ, 3ª Seção, Conflito Negativo de Competência 29.886/SP, rel. Min. Maria Thereza de Assis Moura, DJ 1º-2-2008).

NOTIFICAÇÃO POR E-MAIL

Comentários:

A tendência é o uso cada vez mais intenso dos meios eletrônicos para a comunicação em geral. Por excelência, o meio mais comum é o *e-mail*. Todavia, para que tal meio tenha maior força probatória, é necessária a utilização de assinatura digital, principalmente quando se tratar de comunicação com efeitos jurídicos.

A assinatura digital, de maneira simplista e resumida, serve para atestar a autenticidade do emitente da declaração, tornando válida a autoria da mensagem.

“Apelação cível. Responsabilidade civil. Ação de rescisão contratual cumulada com pedido de dano moral e sustação de protesto. 1. Sentença extra petita é aquela que decide fora dos limites do pedido, situação não configurada na hipótese dos autos. 2. Para que ocorra a rescisão do Contrato de Comercialização de Bilhetes de Passagens Aéreas entabulado entre as partes, imprescindível a notificação específica, não se prestando os e-mails enviados para tal fim, uma vez que estes se destinavam para o pagamento da dívida e manutenção do contrato. 3. Tratando-se de dívida representada por cheques devolvidos sem provisão de fundos, os juros de mora e a correção monetária incidem a partir da apresentação das cédulas ao banco, a teor das disposições do art. 397 do Código Civil vigente, ressaltando que incidirão após

o decreto de falência se o ativo da massa comportar o seu pagamento. Apelo provido em parte. Unânime” (TJRS, Apelação Cível 70028595817, rel. Gelson Rolim Stocker, j. 28-7-2010).

“Apelação cível. Direito privado não especificado. Ação de exibição de documentos. Sentença que não reconheceu a pretensão resistida no plano do direito material. Notificação via e-mail. Presente o interesse de agir do autor, face ao não atendimento de pedido seu realizado na via administrativa e à necessidade de ajuizamento da presente demanda para a obtenção de todas as informações referentes à relação contratual afirmada inverídica e inexistente. É válido o pedido administrativo formulado pela demandante por via eletrônica (e-mail), através de canal disponibilizado pela própria empresa demandada em seu site. Presente a necessidade de ajuizamento de demanda cautelar para a obtenção dos documentos requeridos pela autora. Pretensão resistida verificada. Sentença desconstituída. Apelação provida” (TJRS, Apelação Cível 70033482571, rel. Glênio José Wasserstein Hekman, j. 16-12-2009).

“Administrativo. Contrato privado da administração sob a égide do direito privado. Inteligência da Lei n. 9.656/98 e da Lei n. 8.078/90. Impossibilidade de exclusão unilateral de dependentes indiretos pela operadora de plano de saúde privado. Recursos improvidos. 1. No caso dos autos é questionada a exclusão dos dependentes indiretos do seguro saúde coletivo da Sul América Saúde Ltda., contratado pelo Ministério da Agricultura, através de processo licitatório. 2. Os contratos privados da Administração Pública têm regime especial que utiliza regras do Direito Privado. Ou seja, ainda que os princípios dos contratos administrativos e dos contratos de direito privado praticados pela Administração sejam os mesmos, as regras aplicáveis a esses últimos não são as mesmas aplicáveis nos contratos administrativos. 3. A Lei impõe vedação às operadoras de saúde quanto à suspensão ou rescisão unilateral dos contratos, principalmente em razão da idade avançada dos segurados. 4. A questão também se subordina as normas do Código de Proteção e Defesa do Consumidor — Lei n. 8.078/90, que assegura ao consumidor o direito de informação, conforme dispõe em seu art. 6º. No art. 51 o CDC também dispõe que ‘são nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: (...) XI — autorizem o fornecedor a cancelar o contrato unilateralmente, sem que igual direito seja conferido ao consumidor;’ 5. Portanto, conclui-se que caberia à operadora de saúde comunicar previamente da exclusão das seguradas. E não há comprovação que esta comunicação via Internet tenha chegado às autoras. Destarte, a pretensão autoral merece acolhimento. 6. Recursos improvidos” (TRF2, Petição 2003.51.01.021149-3, rel. Guilherme Calmon Nogueira da Gama, publ. 26-8-2009).

“Agravado de instrumento. Ação de rescisão contratual c/c cobrança e pedido liminar de antecipação de tutela. Manifestação de renúncia dos patronos da agravante. Comprovação da ciência inequívoca da outorgante. Inexistência. Manutenção da representação até o julgamento do agravo. Possibilidade. Pretensão de pagamento dos aluguéis não demonstrada. Devolução dos bens locados pela agravante. Possibilidade. Capacidade de pagamento da empresa comprometida. Risco de lesão grave ao agravado. Multa em patamar elevado. Redução. Princípios da razoabilidade e proporcionalidade. Possibilidade. Recurso parcialmente provido. A manifestação de renúncia, juntada aos autos pelos patronos da agravante, necessita de comprovação da ciência inequívoca da outorgante, que deve ser feita pelo advogado-renunciante. O simples comunicado por e-mail, sem comprovação de seu recebimento e ciência pelo representante da agravante, não tem o condão de produzir os efeitos processuais pretendidos. A sociedade empresária agravante, em situação de incapacidade de pagamento, além de suspeita de fraude à economia popular, noticiada pela imprensa, não demonstrou qualquer intenção de quitar seus compromissos financeiros com o agravado, ou ainda, de dar continuidade às suas atividades sociais, de forma a possibilitar a recuperação de sua capacidade de pagamento. De sorte que, diante do perigo de lesão grave, de difícil ou incerta reparação ao agravado, e das informações prestadas pelo d. magistrado primevo, ao que tudo indica, não há qualquer intenção da empresa em pagar seus credores, ainda que continue na posse dos bens locados, o que impõe a manutenção da decisão de primeiro grau que concedeu a antecipação de tutela requerida pelo agravado. Se a multa cominatória revela-se excessiva, em atenção aos princípios da razoabilidade e da proporcionalidade, o magistrado pode, de ofício, reduzi-la a patamares mais ajustados à realidade econômica das partes” (TJMG, Recurso Cível 9268322-40.2009.8.13.0079, rel. Eduardo Mariné da Cunha, j. 21-5-2009).

PRINCÍPIO DA PUBLICIDADE E INTERNET

Comentários:

A Internet pode ser considerada um dos meios de se efetivar a transparência na Administração Pública. Por outro lado, a Internet ainda não pode ser considerada um meio que vá atingir toda população, já que no Brasil nem todos possuem acesso à rede mundial de computadores.

Dada essa dicotomia, selecionamos algumas decisões judiciais que tratam sobre o tema.

“Tributário e processual civil. Mandado de segurança. Simples nacional. LC n. 123/2006. Exclusão pela Internet. 1. Não poderão recolher os impostos e contribui-

ções na forma do Simples Nacional empresas que possuam débito com a Fazenda Pública. Dicção do art. 17, V, da Lei Complementar n. 123/2006. 2. Nos processos de exclusão de ofício do Simples, o procedimento a ser adotado é aquele relativo ao processo administrativo fiscal da entidade que está a proceder a exclusão, conforme o § 5º, sendo que a ciência da exclusão deverá observar também essa legislação, segundo regra estampada no § 3º da Resolução n. 15, de 15-7-2007, do CGSN. 3. A publicação na Internet, de que trata o § 4º do ato regulamentar, é condição necessária para eficácia do ato de exclusão, em face do princípio da publicidade dos atos da administração, não sendo, entretanto, o meio válido de notificação do contribuinte, porquanto a notificação, nos termos do próprio ato regulamentar, há de ser feita conforme a legislação que rege o processo administrativo fiscal do ente federal responsável pelo processo de exclusão, que, no caso da União, é o Dec. N. 70.235, de 1972. 4. Apelo provido” (TRF4, Mandado de Segurança 2009.71.08.004618-2, rel. Luciane Amaral Corrêa Münch, j. 20-4-2010).

“Embargos à execução fiscal. Indeferimento da adesão ao REFIS. Excesso de execução não comprovado. Regularidade da CDA. 1. A publicação na Internet do indeferimento da adesão da empresa do Programa de Recuperação Fiscal é suficiente para que o contribuinte tome conhecimento de sua situação perante o Fisco e possa providenciar sua defesa, não havendo afronta aos princípios constitucionais do devido processo legal, do contraditório e da ampla defesa. 2. A arguição de nulidade da CDA deve vir acompanhada de prova inequívoca de sua ocorrência, não se mostrando suficiente para o afastamento de sua presunção de certeza e liquidez (nos termos do art. 3º da Lei n. 6.830/80 — LEF) mera afirmação de que os dados nela insertos não estão corretos ou são incompreensíveis. 3. Inexistindo comprovação do alegado excesso de execução, permanece hígida a cobrança, face à presunção de certeza e liquidez da CDA” (TRF4, Apelação Cível 2005.72.06.000461-0, rel. Álvaro Eduardo Junqueira, publ. 4-5-2010).

“Administrativo. Auto de infração. Princípio da publicidade. Fato gerador. Descumprimento de obrigação de informar o início do trabalho de pesquisa. Art. 31, parágrafo único, do Regulamento do Código de Mineração. 1. Há que se considerar o princípio da publicidade, o qual impõe à Administração Pública que preste aos administrados as informações completas, claras e acessíveis. Se os contribuintes não foram informados pela forma mais usual, sobre o pagamento de taxa, que é a emissão de boletos bancários via correio, bem como grande parte da população mundial, incluídos os cidadãos brasileiros, não possuem acesso à rede mundial de computadores (Internet), conclui-se que não foi observado o princípio da publicidade de forma devida. 2. Uma vez não atendida obrigação de informar o início do trabalho de pesquisa, incide o disposto no art. 31, parágrafo único, do Regulamento do Código de

Mineração. 3. Apelação parcialmente provida” (TRF4, Apelação Cível 2008.71.00.002793-8, rel. Carlos Eduardo Thompson Flores Lenz, j. 9-6-2010).

PROCESSO DIGITAL. OFENSAS NA INTERNET. COMPETÊNCIA

“Processual civil. Ação de indenização por danos morais. Veiculação de notas na Internet. Foro competente. 1. Produzido o dano em diversos lugares, pela natureza do veículo no qual foi divulgado o escrito tido por ofensivo (Internet), podem as vítimas escolher qualquer dos foros correspondentes, no caso, o do seu domicílio (Precedentes do STJ). 2. Agravo de Instrumento a que se dá provimento” (TRF01, AG 0004619-03.2003.4.01.0000/DF, rel. Maria Isabel Gallotti Rodrigues, publ. 22-2-2010).

“Processo penal. Crimes praticados através da Internet. Competência. Justiça federal. Sentença reformada. 1. A inserção de dados aos crimes relativos ao racismo na rede mundial de computadores — Internet — possibilitando o acesso a qualquer pessoa, em qualquer parte do mundo, tornando-os públicos, determina a competência da Justiça Federal, pois o crime previsto em tratado teve seu resultado, inevitavelmente, ocorrido no estrangeiro. 2. Sendo a União detentora da competência exclusiva para manter relações com os Estados estrangeiros e com eles celebrar tratados e convenções, e o Brasil um dos signatários da Convenção sobre os Direitos da Criança, é a Justiça Federal competente para processar e julgar o crime previsto no art. 241 do Estatuto da Criança e do Adolescente (Lei n. 8.069/90). 3. Recurso em sentido estrito provido” (TRF01, RSE 2008.38.00.018067-7/MG, rel. Juiz Tourinho Neto, publ. 9-10-2009).

“Ação Monitória. Assinatura Digitalizada. Validade. Impugnação que está restrita a forma pela qual foi consignada a assinatura, sem contestação quanto à autenticidade dos documentos. Aplicação do art. 154, CPC. Sistema Processual que enaltece o aproveitamento máximo dos atos processuais. Ato que cumpriu sua finalidade e não causou prejuízos às partes. Decisão mantida. Recurso improvido” (TJSP, Apelação 991.00.067003-7, rel. Des. Paulo Roberto de Santana, j. 9-6-2010).

PECULATO ELETRÔNICO

“Apelação criminal. Peculato eletrônico e formação de quadrilha. Recurso ministerial. Condenação de todos os denunciados. Existência de relevante dúvida

sobre o envolvimento do corréu na empreitada delituosa. Elementos de convicção coligidos nos autos que não se mostram seguros no delineamento da participação do acusado. Absolvição. Possibilidade. Formação de quadrilha. Condenação. Impossibilidade. Ausência de elementar típica. Absolvição mantida. Recurso conhecido e desprovido” (TJRS, Apelação Cível 2921908-09.2004.8.13.0024, rel. Márcia Milanez, j. 28-8-2009).

ESTELIONATO

*“Penal e processo penal. Crimes de estelionato (art. 171 do CP) e extorsão (art. 158 do CP) cometidos pela Internet. Utilização de ardis e artifícios inidôneos para enganar o homem médio. Absolvição. Exigência de vantagem indevida acompanhada de ameaça de divulgação de conversas mantidas em sala de bate-papo de rede social. Configuração do delito. Pena. Consequências. Decote. Vítima que não quer ser ressarcida do prejuízo sofrido. Presunção de irrelevância. Regime. Abrandamento. Provimento parcial. 1. O crime de estelionato pressupõe uma vontade viciada da vítima, que entrega a coisa espontaneamente. O ofendido se equivoca quanto à realidade fática. 2. Qualquer pessoa que frequente sala de bate-papo ou sítios de relacionamentos na Internet sabe que nem sempre as informações passadas em tais redes sociais são condizentes com a verdade. 3. A conduta da ré não se mostra materialmente típica, porque, embora a lei tenha obrigado o estado a tutelar o patrimônio do cidadão, das investidas dos estelionatários, não se preocupou com a utilização de ardis ou artifícios pueris, incapazes de enganar o homem médio. Absolvição decretada. 4. Na extorsão, diversamente, a vítima sabe o que está acontecendo e faz a entrega da coisa contra a sua vontade, em razão de violência ou grave ameaça (art. 158 do CP). 5. Se a ré a passa a exigir, mediante emprego de grave ameaça, novos depósitos em dinheiro em sua conta bancária, sob pena de noticiar os fatos aos jornais, à televisão, à esposa da vítima, aos seus colegas de trabalho, acusando-o de haver praticado o crime de pedofilia, eis que supostamente contava apenas 16 (dezesesseis) anos de idade, incide na figura típica do crime de extorsão (art. 158 do CP). 6. Em relação às consequências do delito, é de se entender que não devem militar em desfavor da ré, haja vista dispensa, pela própria vítima de ressarcimento, indicando que o desfalque, na sua óptica, não foi considerável. 7. Em razão do *quantum* de pena fixado, razoável o estabelecimento de regime prisional menos gravoso. 8. Recurso parcialmente provido para absolver a ré da imputação do crime de estelionato e reduzir as penas impostas, fixando-lhe regime menos gravoso” (DF 0045217-48.2010.807.0001, 2ª Turma Criminal, rel. Silvânio Barbosa dos Santos, j. 26-5-2011, DJe 7-6-2011, p. 208).*

PRONTUÁRIO MÉDICO ELETRÔNICO

“Apelação cível 2 (Município). Ação de retificação de dados cadastrais c/c reparação de danos. Inclusão de CID equivocado em prontuário eletrônico da paciente. Responsabilidade objetiva da administração por imperícia e negligência de seu agente. Informação acessível apenas aos profissionais do sistema de saúde. Propagação de diagnóstico de AIDS no meio social inimputável ao Município. Sentença parcialmente reformada. Recurso provido para reduzir o valor da indenização. I — Responde objetivamente o Município por ato da médica do sistema público de saúde que registra, por equívoco, no prontuário eletrônico da paciente, CID referente à infecção pelo vírus da AIDS. II — À luz do caso concreto, o valor da condenação comporta sensível redução, mormente se a informação era de acesso restrito aos profissionais do sistema de saúde, sendo o equívoco prontamente esclarecido e a propagação da notícia no meio social e familiar da paciente não se deveu à conduta dos agentes do Município. Apelação cível 1. Majoração da verba indenizatória. Recurso prejudicado” (TJPR, Apelação Cível 504.452-0/PR, 0504852-0, rel. Des. Rubens Oliveira Fontoura, j. 14-7-2009).

PUBLICAÇÃO NA INTERNET COMO MEIO DE CIÊNCIA

“Programa de recuperação fiscal. REFIS. Exclusão. Ausência de notificação pessoal. Notificação por meio do diário oficial e da Internet. Possibilidade. REsp 1.046.376/DF. Matéria julgada sob o regime do art. 543-C do CPC. 1. A controvérsia dos autos reside em saber se é legítima a exclusão do contribuinte que aderiu ao REFIS e tornou-se inadimplente, mediante publicação da Portaria no Diário Oficial da União e na rede mundial de computadores — Internet —, ou se seria imprescindível a notificação pessoal. 2. A Primeira Seção do STJ, no julgamento do recurso repetitivo REsp 1.046.376/DF, em 11-2-2009, reafirmou entendimento segundo o qual é legítima a exclusão do contribuinte que aderiu ao REFIS e tornou-se inadimplente, mediante publicação na rede mundial de computadores — Internet. 3. Aplica-se ao caso a multa do art. 557, § 2º, do CPC no percentual de 10% (dez por cento) sobre o valor da causa, por questionamento de matéria já decidida em recurso repetitivo. Agravo regimental improvido” (STJ, 2ª Turma, AgRg no REsp 1.205.170/DF, rel. Min. Humberto Martins, j. 16-8-2011, DJe 22-8-2011).

“Recurso especial. Processo civil. Informações processuais disponibilizadas via Internet. Caráter oficial à luz da Lei n. 11.419/2006. Prestígio à eficácia e confiabilidade das informações prestadas por meio da Internet. Hipótese de erro ou falha do sistema.

Justa causa. Possibilidade de identificação. Conjuntura legislativa e jurisprudencial. Atualidade. Homenagem à adoção de recursos tecnológicos. Melhoria da prestação jurisdicional. Art. 5º, LVXXII, da Carta Republicana. Recurso Especial improvido. I — Com o advento da Lei n. 11.419/2006, que veio disciplinar ‘(...) o uso de meio eletrônico na tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais’, a tese de que as informações processuais fornecidas pelos sites oficiais dos Tribunais de Justiça e/ou Tribunais Regionais Federais, somente possuem cunho informativo perdeu sua força, na medida em que, agora está vigente a legislação necessária para que todas as informações veiculadas pelo sistema sejam consideradas oficiais. II — A razão desta interpretação é consentânea com o art. 4º, *caput* e § 2º da Lei n. 11.419/2006, que expressamente apontam, *in verbis*: ‘(...) Art. 4º. Os tribunais poderão criar Diário da Justiça eletrônico, disponibilizado em sítio da rede mundial de computadores, para publicação de atos judiciais e administrativos próprios e dos órgãos a eles subordinados, bem como comunicações em geral. (...) § 2º A publicação eletrônica na forma deste artigo substitui qualquer outro meio e publicação oficial, para quaisquer efeitos legais, à exceção dos casos que, por lei, exigem intimação ou vista pessoal’. III — A disponibilização, pelo Tribunal, do serviço eletrônico de acompanhamento dos atos processuais, para consulta das partes e dos advogados, impõe que ele se realize de modo eficaz, uma vez que há presunção de confiabilidade das informações divulgadas. E, no caso de haver algum problema técnico do sistema, ou até mesmo algum erro ou omissão do serventário da justiça, responsável pelo registro dos andamentos, que porventura prejudique umas das partes, poderá ser configurada a justa causa prevista no *caput* e § 1º do art. 183 do Código de Processo Civil, salvo impugnação fundamentada da parte contrária. IV — A atual conjuntura legislativa e jurisprudencial é no sentido de, cada vez mais, se prestigiar a divulgação de informações e a utilização de recursos tecnológicos em favor da melhor prestação jurisdicional, com evidente economia de recursos públicos e em harmonia com o que dispõe o art. 5º, LXXVIII, da Carta Republicana. V — Recurso especial improvido” (STJ, 3ª Turma, REsp 1.186.276/RS, rel. Min. Massami Uyeda, j. 16-12-2010, DJe 3-2-2011).

COMPETÊNCIA PARA JULGAMENTO DE OFENSAS NA INTERNET

“Agravamento regimental em agravo de instrumento contra a inadmissão de recurso especial. Ação de indenização por danos morais. Juízo competente. Art. 100, V, ‘a’, do CPC. Lugar do ato ou fato. Local em que se irradiam os efeitos da notícia veiculada via internet. Agravo regimental desprovido. 1. O Tribunal a quo decidiu a lide de acordo com o entendimento desta Corte, no sentido de que, nas ações em que se discutem danos morais praticados por meio de comunicação de grande circulação, impõe-se

a aplicação da regra prevista no art. 100, V, ‘a’, do CPC. Deve ser considerado o ‘lugar do ato ou fato’ aquele em que a notícia irá produzir maior repercussão, no caso, a cidade de Barretos, onde se localiza a sede da ora agravada, entidade que organiza o principal rodeio do país e que se reputa ofendida pelas notícias veiculadas pela organização não governamental de proteção aos animais ora agravante. 2. Agravo regimental a que se nega provimento” (AgRg no Ag 1.118.840/SP, 4ª Turma, rel. Min. Raul Araújo, j. 5-5-2011, DJe 7-6-2011).

COMPETÊNCIA PARA APURAÇÃO DE CRIMES NA INTERNET

“Conflito negativo de competência. Penal e processual penal. Comercialização de DVDs falsificados. Violação de direitos autorais. Art. 184, § 2º, do Código Penal. Incompetência do juízo federal. Ausência de indícios da internacionalidade da conduta. Conflito conhecido para declarar a competência do juízo de direito da 2ª Vara de Direito Criminal e de Execuções Penais da Comarca de Conselheiro Lafaiete/MG, o suscitado. 1. A conduta de comercializar obras artísticas falsificadas (DVDs) caracteriza o delito de violação de direito autoral, em atenção ao princípio da especialidade. Não havendo notícia da ocorrência de comercialização do produto além das fronteiras, afastada está a competência da Justiça Federal para o exame do feito. A mera divulgação da venda por meio da Internet, *tout court*, não tem o condão de conduzir ao reconhecimento da transnacionalidade, e, via de consequência, a competência de Justiça Federal. 2. Conflito conhecido para determinar competente o suscitado, Juízo de Direito da 2ª Vara Criminal e de Execuções Penais de Conselheiro Lafaiete/MG” (STJ, 3ª Seção, CC 116.820/MG, rel. Min. Maria Thereza de Assis Moura, j. 10-8-2011, DJe 18-8-2011).